방송통신정책연구 11-진흥-라-08

모바일 보안시장 생태계 조성을 위한 환경구축 연구

(A Study on Mobile Security Ecosystems)

정동길/오민진/장정우/조아라

2011.12

연구기관: 명지대학교

방송통신위원회
KOREA COMMUNICATIONS COMMISSION

제 출 문

방송통신위원회 위원장 귀하

이 보고서는 2011년도 방송통신위원회 방송통신발전기금 방송통신정책연구사업의 연구결과로서 보고서의 내용은 연구자의 견해이며, 방송통신위원회의 공식입장과 다를 수 있습니다.

본 보고서를 『**모바일 보안시장 생태계 조성을 위한 환경구축 연구**』의 연구결과보고서로 제출합니다.

2011년 12월

연구기관: 명지대학교
총괄책임자: 정 동 길
참여연구원: 오 민 진
참여연구원: 장 정 우
참여연구원: 조 아 라

목 차

표 목 차

그 림 목 차

요 약 문

1. 제 목

모바일 보안시장 생태계 조성을 위한 환경구축 연구

2. 연구 필요성 및 목적

스마트폰과 태블릿 PC로 불리는 스마트 모바일/미디어 시대가 현실화 되어가면서 모바일 보안이 다시금 세간의 주목을 받기 시작했다. 이미 많은 전문가들은 한국도 모바일 보안에 대해 안전할 수 없다고 여러 차례 강조해 왔고, 모바일 보안 위협이 증가할 것이란 통계들도 속속 보고 되고 있다. 모바일 기기와 서비스의 폭발적인 증가로 국내에서뿐만 아니라 해외에서도 이미 다양한 형태의 모바일 바이러스가 큰 혼란을 야기시키는 일이 비일비재하게 일어났다.

스마트 모바일은 이미 일반 PC와 유사할 정도로 기능이 향상되었지만, 기능의 향상과 더불어 일반 PC 만큼의 정보보안 위협에도 직면하고 있다. 그럼에도 불구하고 국내 스마트 모바일은 아직 개화기의 단계이기 때문에 보안보다는 진흥에 초점이 맞춰져 있다. 모바일 보안 침해행위는 실시간성과 동시성, 비대면성과 익명성, 광역성 내지 국제성, 범죄영역의 무한대성, 전파의 신속성과 피해의 대규모성, 범행의 반복성, 범죄적발 및 입증의 곤란과 손해배상의 어려움 등의 속성이 있다.

우리나라 모바일보안 산업의 가장 큰 약점은 그 가치사슬에 참여

하는 산업계의 상호협력 또는 자생적 생태계가 안정화되지 않았다는 것이다. 모바일 보안대책이 문제발생시마다 즉흥적 대책이 아닌 구조적이고 조직적인 해결체계를 가지기 위해서는 국가적인 차원에서 모바일 보안 생태계 구축이 시급하고 스마트폰 보급 확산단계인 지금이 모바일 보안 생태계 형성과 대책 수립의 적기라고 보여진다.

3. 연구의 구성 및 범위

본 연구의 구성은 다음과 같이 정리될 수 있다. 첫째, 모바일 보안 산업/시장 동향 분석 및 전망을 한다. 건전한 모바일 산업 생태계를 구축하기 위해서는 모바일 보안산업이 태어난 배경과 현재 진행되고 있는 상황에 대한 자료 수집과 분석이 필요하다. 이를 바탕으로 앞으로 전개될 모바일 보안시장에 대한 예측해 본다. 이 예측은 국내 시장과 외국시장으로 나누어서 실시하되 외국 시장의 경우 앞으로 우리나라가 진출을 시도해 볼 가치가 크다고 판단되는 중국 시장에 대해서는 상대적으로 깊고 자세한 시장 분석을 한다.

둘째는 모바일 보안산업 경쟁력 육성 및 제고를 위한 핵심기술 R&D 및 기술 수요 실태조사·분석을 한다. 모바일 보안 시장과 산업은 그 속성상 범용 운영체제(Operating System)가 탑재된 스마트폰의 탄생이후 형성되고 있기 때문에 본격적인 모바일 보안시장의 탄생과 형성은 불과 2~3년전에 시작되었고 이제 태동기에 있다고 볼 수 있다. 따라서 모바일 보안 시장은 우리에게 특히 소프트웨어 기술과 시장에서 주도권과 경쟁력을 가지고 진출할 수 있는 좋은 기회이다. 이를 위해서는 먼저 모바일 보안산업에서의 핵심기술을 파악하고 이에 대한 연구개발을 선도적으로 시도해야 할 필요가 있다. 현실적으로 모바일 보안 핵심기술에 대한 연구개발 정보는 연구개발 주체뿐 아니라 보안산업 관련 종사자들에게 매우 민감하고 획득하기 어려운 관계로 이에 대한 실태조사와 분석은 한계를 가지고 있다.

셋째, 우라니라 모바일 보안산업에 관여하는 대기업, 중소기업, 소비자, 정부 등 시장의 각 주체들이 상호 발전을 하기 위한 모바일 보

안시장 상생 프레임워크를 구축하는 방안에 대한 정책적 제언을 제공하는 것이다. 우리나라가 21세기 지구촌의 새로운 키워드인 디지털 융합과 유비쿼터스 사회에 있어서 핵심인 모바일 소프트웨어 플랫폼과 모바일 보안산업의 경쟁력을 확보하기 위해 국가적으로 어떤 전략을 택해야 하며 이러한 전략을 수행하기 위한 정부차원에서의 정책적 방안을 논의하는 것이 중요하다. 본 연구에서는 모바일 보안 시장을 소프트웨어 플랫폼 기반의 다면 플랫폼 시장으로 파악하고 관련된 산업 네트워크들이 서로 밀접하게 상호 작용하면서 하나의 생태계를 형성하여 진화해 산업이라는 공생적 프레임워크로 파악한다. 이렇게 어떤 플랫폼을 중심으로 관련 산업 네트워크가 밀접하게 상호작용하며 움직이는 산업 생태계가 국가적 차원의 경쟁력을 가지기 위해서는 무엇보다도 정부차원에서 지향해야 할 바른 방향의 지표들을 제시하고자 한다.

정리하면 본 연구에서는 다음 사항에 대한 연구를 수행한다.

- 모바일 보안 산업/시장 동향 분석 및 전망
  - 모바일 보안 정책 및 전략수립 지원을 위한 국내 모바일 보안 산업 현황 및 시장규모 분석
  - 해외 주요국 모바일 보안 산업 현황 및 시장 규모 분석
  - 해외 주요 모바일 보안기술 현황 조사 및 트랜드 분석
- 모바일 보안산업 경쟁력 육성 및 제고를 위한 핵심기술 R&D 및 기술 수요 실태조사·분석
- 대기업, 중소기업, 소비자, 정부 등 시장의 각 주체들이 상호 발전을 하기 위한 상생 프레임워크 구축 방안 마련
  - 국내외 모바일 보안 산업 지원 정책의 비교 분석
  - 모바일 보안 산업 육성 방안 마련
  - 모바일 보안시장 확대 및 수출전략 등 전략적 육성 방안

4. 연구 내용 및 결과

첫째, 모바일 보안 산업/시장 동향 분석 및 전망의 결과는 다음과 같다. 먼저 모바일 보안시장/산업에 대하여 현재까지 통일된 정의나 개념정립은 이루어지지 않고 있다. IDC와 같은 주요 IT 시장조사기관에 의하면 모바일 보안시장/산업은 전통적인 유선 네트워크에 연결되는 PC와 고정 네트워크 기반시설(Fixed Network Infrastructure)에 발생하는 보안문제는 그 대상에서 제외하고 모바일 전화기, 스마트폰, 태블릿 PC, PDA, RFID, 무선센서 등 현대적인 의미의 모바일 기기에서 발생하는 보안문제를 해결하기 위한 소프트웨어/하드웨어 제품이라는 기본 개념을 공통분모로 하여 모바일 보안시장에 대한 시장조사와 시장예측을 위한 접근방법을 취하고 있다.

국내 모바일 보안시장의 경우 2010년 총 1조원의 정보보안 매출액 중 무선·모바일 부문이 전년대비 가장 높은 증가율을 보였으며 전년대비 79.3% 성장한 266억원을 기록했다. 무선·모바일 보안 시장은 연평균 13.7%의 성장률을 보이며 2015년경 506억원대의 시장을 형성할 것으로 조사됐다. 특히 이 시장은 최근 스마트폰과 아이패드 등의 열풍으로 인해 큰 성장을 이를 수 있을 것으로 예상됐다.

중국시장의 경우 스마트폰의 대중화에 따른 모바일 보안용 SW 수요의 증가, 정부당국의 관련정책, 3G 및 모바일 인터넷의 지속적인 성장, 바이러스로 인한 크고 작은 보안사고, 사용자들의 보안에 대한 인식도 등은 저마다 모두 모바일 보안산업의 향방에 영향을 미칠 것이다. 모바일 보안산업 발전의 제반 환경에 대한 분석을 바탕으로 프로스트&설리번은 2010년 말 모바일 보안제품 활성 사용자가 7천 2백만명을 넘을 것으로 추산했으며, 시장규모는 계속해서 빠르게 확대될 것으로 전망한다. 2014년에는 중국 내 모바일 보안제품 활성 사용자 비중이 전체 사용자의 85%에 달할 것으로 예상되고 있으며, 실사용자 수는 약 4억 3천 4백만명에 이를 것으로 전망된다.

글로벌 모바일 보안시장의 경우 저명한 시장조사기관인 IDC에 따르면 2015년 전 세계 모바일 보안시장은 190억 달러 규모로 2010년의

4억700만 달러에서 비약적인 성장을 기록할 것으로 전망되고 있다. 이중 DLP (Data Loss Prevention)와 Encryption을 포함한 Mobile IPC (Information Protection and Control), MIAM (Mobile Identity and Access Management), MSVM (Mobile Security and Vulnerability Management), Mobile Threat Management, Mobile VPN(Virtual Private Network) 등이 2010년부터 2015년 사이에 연간 평균 30% 이상의 성장률을 보일 것으로 예측되었다.

둘재, 모바일 보안산업 경쟁력 육성 및 제고를 위한 핵심기술 R&D 및 기술 수요 실태조사·분석의 결과는 다음과 같다. 먼저 모바일 보안 기술분야는 크게 나누어 Wireless Communication 일반, USN 보안, 클라우드 컴퓨팅 보안, 모바일 오픈마켓과 콘덴츠 보안, 그리고 Mobile Device 보안과 같은 5개의 분야로 나누어 살펴볼 수 있다.

Wireless Communication 일반의 경우, 무선 환경의 문제는 유선통신에 비해 기술적으로 완벽히 보안문제를 해결할 수 없다는 사실이다. 최대한 피해를 최소화 하는 것이 중요하며 적절한 암호화와 인증기술올 활용하면 상당한 수준으로 해결이 가능하다. 특히 모바일 디바이스를 위한 경량 SSL 기술은 매우 중요하다. 전송 송출 수준을 감소시키거나 이에 해당하는 기술을 개발하는 것도 중요하고. 주파수 도약(Frequency Hopping Radio) 기술을 사용하여 전파 방해나 다중경로 페이딩(Multi-path Fading)을 방지하는 것도 하나의 방법이다.

USN 보안이슈와 관련하여 본연구에서는 영향도와 사회적 비용, 발생가능성 등은 상대적으로 다른 보안이슈에 비해 낮은 것으로 나타났다. 이러한 결과는 다른 보안이슈에 비해 USN보안이슈가 상대적으로 보안상의 문제점올 일으킬 가능성이 적다는 것올 의미한다, 하지만 소형기기를 감염시켜 악성코드를 유포시키는 기술이 더욱 발전한다면 매우 큰 문제가 될 수 있음으로 주의가 필요할 것이다,

다양한 보안기술을 개발하려는 시도가 예상되는 가운데 클라우드 컴퓨팅 서비스 제공자들에서 보안은 클라우드 서비스의 핵심과제로 인식하게 만드는 것이 매우 중요하다. 업체들이 수익만올 고려하지 않고 실시간으로 모니터링 시스템올 갖추고 l, 데이터에 대한 암호화

및 백업 작업을 게을리 하지 않는다면 위협은 많이 감소할 것이다. e-Discovery기술, 대용량 패킷처리가 가능한 침입탐지기술(IDS), 개인인증, 개인정보보호, 접근통제를 이용한 기업 데이터 보호기술 등도 더욱 개발할 필요가 있다. 클라우드 컴퓨팅 보안이슈의 발생가능성을 국내와 해외로 비교해서 살펴보면 국내보다는 해외의 클라우드 컴퓨팅 서비스 보급률이 훨씬 높기 때문에(예컨대, 아마존 서비스) 해외에서 먼저 문제가 발생할 소지가 높다. 그러므로 대부분의 서비스는 외국회사가 중심이 될 것으로 보이며 국내에서는 외국에서 문제가 발생하고 어느 정도 보안문제가 해결된 후 본격적으로 활성화 될 가능성이 높다.

모바일 오픈마켓도 많은 사용자들이 접근함으로 보안문제가 발생할 것이다. 이러한 문제를 해결하기 위해서는 우선 앱스토어 내의 검증을 강화하여야 한다. 앱스토어 운영자는 안전성이 확보된 코드를 이용한 앱을 유통시켜야 하며 보안에 허점이 있거나 불건전한 앱의 유통은 철저히 근절할 필요가 있다. 또 정보의 유출이나 공유에 대한 적절한 관리와 데이터에 대한 합법적인 권한에 대한 기술도 필요하다. 무선기기의 증가 및 기능 향상에 따른 상호인증 기술 및 안전한 코드 개발 기술도 필요하다. 현재 국내에서는 콘텐츠 공유에 대해서는 별다른 법적 조치나 대응이 없다. 콘텐츠 보안문제를 근본적으로 해결하는 것은 거의 불가능하고 개별적으로 막기가 매우 힘들기 때문에 적극적인 관심과 대응이 필요한 실정이다. 다만 DRM 등의 기술을 강화하는 등의 조치는 필요하다.

모바일 디바이스는 분실, 악성코드 감염, 정보유출, 금전적 손실, 공격지 활용 등 여러 가지 위협요인을 가지고 있다. 아무래도 개인용 컴퓨터에 비해 연산능력이나 전원 지구성 등 시스템의 완결성 측면에서 부족해 보안에 취약성을 크게 가지고 있다. 특히 악성 소프트웨어를 통한 공격에 노출될 가능성이 큰데 윈도우기반 모바일 기기나 안드로이드 기반의 스마트폰의 경우 검증되지 않은 앱을 위장하여 사용자의 주소록, 통화기록, 문자 메시지 등을 빼돌리는 등의 사고가 급증하고 있다. 또 모바일 기기 사용량이 많은 만큼 네트워크의 복잡성이

야기되어 문제발생시 피해액도 클 것으로 예상된다. 위치정보를 비롯한 개인정보의 유출 등도 쉽게 생각해 볼 수 있는 문제다. 이러한 문제점을 해결하기 위해서는 네트워크 설계 단계부터 보안이슈를 고려하여 설계할 필요가 있다. 이동단말과 네트워크간 암호화 및 단말인증, 제어기술이 좋은 예이다. 또한 구표준으로 구동되는 대량의 단말기와 AP들에 대해 펌웨어 패치를 설치하면 상대적으로 적은 비용으로 이에 대한 대비를 할 수 있다.

셋째, 대기업, 중소기업, 소비자, 정부 등 시장의 각 주체들이 상호 발전을 하기 위한 상생 프레임워크 구축 방안 마련에 대한 연구결과는 다음과 같다.

생태계 관점에서 우리나라 모바일 보안산업을 발전시키기 위해서는 1) 수평적 생태계 조성, 2) 경쟁우위 산업 부문에 대한 경쟁력 유지, 3) 취약 부문의 성장 및 발전을 통한 생태계 균형 발전이라는 세 가지 차원에서 점검할 필요가 있다. 생태계의 수평화는 혁신을 위한 환경 조성에 가장 근본적인 요소로, 이를 위해서는 지배적 대형 사업자와 소형 협력사 간의 고질적인 불공정 거래의 관행을 개선시키는 것이 가장 중요하고 시급한 사안이다.

5. 정책적 활용 내용

생태계 관점에서 우리나라 모바일 보안산업을 발전시키기 위해서는 1) 수평적 생태계 조성, 2) 경쟁우위 산업 부문에 대한 경쟁력 유지, 3) 취약 부문의 성장 및 발전을 통한 생태계 균형 발전이라는 세 가지 차원에서 점검할 필요가 있다. 생태계의 수평화는 혁신을 위한 환경 조성에 가장 근본적인 요소로, 이를 위해서는 지배적 대형 사업자와 소형 협력사 간의 고질적인 불공정 거래의 관행을 개선시키는 것이 가장 중요하고 시급한 사안이다.

소프트웨어 부문에서의 경쟁력 강화를 통한 모바일 보안산업 생태계 균형 발전은 향후 ICT 시장에서 소프트웨어 부문의 중요성과 성장

가능성으로 미루어 보아 장기적 관점에서 반드시 중점적으로 간주해야 할 요소이다. 다만, 현재 우리나라의 소프트웨어 부문에서의 기술경쟁력 및 시장 규모가 글로벌 시장에서의 선진국에 비해 뒤처지고 있는 현실을 고려하여 제도적 지원이 뒷받침될 필요가 있다. 규모가 작은 소프트웨어 기업들의 비즈니스를 활성화시키기 위해 M&A에 따른 청산소득금액에 대한 세율을 인하하거나, 초기단계에서의 기업 투자를 촉진하기 위해 엔젤 투자에 대한 세제 지원책을 마련하는 일, 그리고 인터넷 벤처 기업의 인력난 해소를 위해 병역특례 요건을 완화하는 등의 제도적 지원을 하는 것은 소프트웨어 관련 기업 육성에 긍정적으로 기여할 수도 있다.

6. 기대효과

정책적으로 모바일 보안 시장의 상생협력적인 생태계 구축을 위한 정책 지원체계 마련하는데 기여한다, 경제·사회적으로는 미래의 국가성장동력중의 하나인 보안소프트웨어산업과 관련산업의 활성화, 건전한 콘텐츠의 공정한 유통문화 정착, 정보보호 및 관련 서비스산업활성화로 고용기회 증진, 우수한 품질의 보안소프트웨어기술과의 수출과 해외보급으로 국가홍보 및 국가브랜드 이미지 상승에 기여한다.

SUMMARY

1. Title

A Study on Mobile Security Ecosystems

2. Objectives and Importance of the Research

The biggest weakness of the mobile security industry in Korea is that the spontaneous cooperation of the firms that participate in the value chain of the industry, or the ecosystem of the industry has not been stabilized. The measures for the mobile security problems so far have been based on ad hoc manners rather than on systematic and organizational ones. For Korea to have such solid and permanent mobile security solutions, we need to build a healthy mobile security ecosystem at the national level and now it is the best time to do it when Korean people begin to adopt and use smart mobile phones in spread dissemination stage.

3. Contents and Scope of the Research

• Mobile Security Industry / Market Trend Analysis and Forecast

– The analysis of the domestic mobile market status and growth capacity for supporting right and timely establishment of Korean

mobile security industy policies and strategies

– The survey of overseas mobile security industry market status and analysis

• Mobile Security Technology Overseas Research and Trend Analysis

– The analysis of the Research and Development activities and the demand for the mobile security technologies

– Finding out key technologies to develop and enhance a competitive mobile security industry

• Finding out a mutual win-win framework of the mobile security industry where all principal market paricipants such as large corporations, small businesses, consumers and government can coevolve and get benefits from each other

– Comparison of the domestic and foreign industrial policies that promote the mobile security industry support

– Mobile Security industry development plan prepared

– The mobile security market expansion and strategic development plan, including export strategies

4. Research Results

• Mobile Security Industry / Market Trend Analysis and Forecast

• Mobile Security Technology Overseas Research and Trend Analysis

• Finding out a mutual win-win framework of the mobile security industry where all principal market paricipants such as large corporations, small businesses, consumers and government can coevolve and get benefits from each other

5. Policy Suggestions for Practical Use

For the development of a strong mobile security industry in Korea in terms of ecosystem, we need to examine the industry in terms of the three dimensions, 1) the horizontal composition of ecosystems, 2) a competitive advantage for industry to remain competitive, and 3) weak sector's growth and development through the development of ecological balance. To create an environment for the industry-wide innovation, levelization in the industrial ecosystem is the most required fundamental factor and an urgent and sustaining policy commitment for that is to correct unfair trade practices between dominent players and weak and small contracting partners in the market.

6. Expectations

This research provides some inputs to policy derivation for the Korean mobile securty indsutry.

CONTENTS

제1장 서 론

1. 문제의 제기

스마트폰과 태블릿 PC로 불리는 스마트 모바일/미디어 시대가 현실화 되어가면서 모바일 보안이 다시금 세간의 주목을 받기 시작했다. 편하고 생산성을 높여준다는 모바일이지만 치솟는 인기만큼이나 새로운 문제들도 등장하고 있다. 그 중 하나가 모바일 보안이다. 정보보안시장 전망에서 빠지지 않고 등장했던 것이 바로 모바일 보안 위협에 대한 내용이다.

이미 많은 전문가들은 한국도 모바일 보안에 대해 안전할 수 없다고 여러 차례 강조해 왔고, 모바일 보안 위협이 증가할 것이란 통계들도 속속 보고 되고 있다. 특히 스마트폰을 비롯한 다양한 모바일 기기가 출시되는 올해(2011년)에 모바일 기기를 겨냥한 보안 위협이 지난해보다 3배가량 늘어날 전망을 내놓고 있다. 올해 나타난 모바일 악성코드만 해도 1천여건의 유포 사례가 있었으며 7월 이후 그 증가세는 약 2배에 이르고 있다.[1)]

이제 스마트폰은 해커들의 주요 타깃으로 자리매김했다. 기기안에 많은 데이터가 저장돼 있을 뿐만 아니라 스마트폰을 이용해 결제가 가능하며 일반 PC만큼 보안이 잘 돼 있지 않기 때문이다. 2011년은 그야말로 '모바일 악성코드의 한해'였다고 할 만큼 보안 위협에 많이 노출됐지만 2012년은 더욱 심각해질 것으로 전망되고 있다. 모바일 기기와 서비스의 폭발적인 증가로 국내에서뿐만 아니라 해외에서도 이미 다양한 형태의 모바일 바이러스가 큰 혼란을 야기시키는 일이 비일비재하게 일어났다. 올해들어 신종 악성코드들이 맹위를 떨치

---

1) www.boannews.com 2011년 12월 26일자 기사

는 현상이 가중되고 있어 걱정의 목소리가 높은 것이다. 예를 들어 글로벌 보안 기업인 안철수 연구소(대표 김홍선, www.ahnlab.com, 약칭 '안랩')는 2012년 1월 5일 2011년에 발생했던 주요 스마트폰 악성코드 트렌드와 2012년에 예상되는 스마트폰 보안 위협을 발표했다.[2)]

이에 따르면 2011년의 주요 이슈는 ▶과금형 악성코드 폭발적 증가 ▶유명 어플리케이션으로 위장한 악성코드 ▶사생활 침해형 어플리케이션 증가 ▶ 온라인뱅킹정보 노리는 악성코드 발생 등을 꼽았다. 또한, 2012년 한 해 예상되는 주요 스마트폰 보안이슈는 ▶ 어플리케이션, OS 취약점 등을 이용한 악성코드 대량 유포 가능성 ▶커널을 공격하는 루트킷 기능의 발전 ▶ 좀비폰 및 봇넷 본격적 활성화 ▶국내를 겨냥하는 모바일 악성코드 등장 등이다.

2. 연구의 필요성

앞에서 언급한 바와 같이 스마트 모바일에 대한 전자적 침해의 위협으로 인하여 스마트 모바일 정보보안이 시급하지만, 스마트 모바일을 이용하는 대부분의 이용자들이 정보보안 문제를 자각하지 못하고 있다. 스마트 모바일은 이미 일반 PC와 유사할 정도로 기능이 향상되었지만, 기능의 향상과 더불어 일반 PC 만큼의 정보보안 위협에도 직면하고 있다. 그럼에도 불구하고 국내 스마트 모바일은 아직 개화기의 단계이기 때문에 보안보다는 진흥에 초점이 맞춰져 있다. 모바일 보안 침해행위는 실시간성과 동시성, 비대면성과 익명성, 광역성 내지 국제성, 범죄영역의 무한대성, 전파의 신속성과 피해의 대규모성, 범행의 반복성, 범죄적발 및 입증의 곤란과 손해배상의 어려움 등의 속성이 있다. 그러므로 단 한 번의 전자적 침해로 막대한 피해를 유발시킬 수 있다는 점을 유념해야한다. 1개의 악성코드만으로 155대의

2) www.newswire.co.kr 2012년 1월 5일자 기사

스마트폰을 감염시킨 국내의 사례에서도 이 같은 사실을 확인할 수 있다.

스마트 모바일에 대한 전자적 침해가 개인에 대하여 타켓팅되면서 개인에게 정보보안에 적극적으로 대처할 것을 요구하고 있지만, 개인이 다수의 다양한 전자적 침해행위를 적극적으로 차단하기에는 한계가 있다. 그러므로 개인의 정보를 보호하기 위해서 국가 또는 단체 차원의 적극적인 노력이 필요하다.

이에 따라 방송통신위원회를 필두로 하여 정부는 '무선인터넷 활성화 종합계획'에서 스마트 모바일에 대한 보안 강화계획을 발표하였다. 보안위협에 대한 정보공유 및 유관기관간 공조체계 구축 등을 통한 신속한 공동대응체계로서 민관합동대응반을 구성 및 운영하고, 모바일 침해사고에 대응하기 위해 이동통신사, 백신개발자 등 유관기관간 공동대응 훈련 실시 등을 그 내용으로 하고 있다. 따라서 비록 스마트 모바일이 발전 초기 단계일지라도, 정보보안에 대한 국가적·조직적 · 개인적 관심이 필요하다. 이를 위하여 국가 및 공공기관은 스마트 모바일 정보보안에 대한 대응정책을 구상하여야 하고, 기업 및 단체들은 정부의 보안정책을 시행할 여건을 조성하여야 하며, 개인은 이 같은 노력을 적극적으로 수용할 수 있도록 보안에 대한 인식전환을 하여야 한다.

본 연구보고서의 후반부에서 살펴보겠지만 우리나라 모바일보안 산업의 가장 큰 약점은 그 가치사슬에 참여하는 산업계의 상호협력 또는 자생적 생태계가 안정화되지 않았다는 것이다. 모바일 보안대책이 문제발생시마다 즉흥적 대책이 아닌 구조적이고 조직적인 해결체계를 가지기 위해서는 국가적인 차원에서 모바일 보안 생태계 구축이 시급하고 스마트폰 보급 확산단계인 지금이 모바일 보안 생태계 형성과 대책 수립의 적기라고 보여진다. 특히, 우리나라 모바일 보안전반을 고려한 모바일 전자정부 도입은 모바일 생태계 발전에 큰 역할을 제공하는 선순환 구조의 시발점이 될 수도 있다. 즉 모바일 정보보호의 핵심 요소 확립으로 모바일 서비스 사용환경을 위한 정보보호 기반을 강화할 수 있다는 것이다. 이를 위해 지금까지의 기존연구는 주로 모

바일보안에 관련된 개별적인 참여자의 개별적인 대책과 해결책을 제시하는데 머무르고 있는 한계를 가지고 있다. 모바일 보안 생태계 구축을 위해서는 어느 한 영역 또는 분야에서의 보안 대책 수립만으로는 진정한 의미의 모바일 보안 생태계 구축이 어렵다. 우리나라에서 건강한 모바일 보안 산업 생태계의 구축을 위해서는 모바일 보안과 관련된 모든 영역·분야에서 상생적이고 상호보완적인 모바일 보안 산업 생태계 구축을 지원할 수 있는 정부차원에서의 대책을 실증적인 연구와 분석이 필요하다.

이러한 상생 프레임워크 구축의 필요성은 글로벌한 차원에서 모바일 보안 산업을 보면 보안시장 본격화된 모바일 보안침해에 대응하기 위해 많은 보안 제품과 서비스들이 출현하고 있으나 최근 악성 코드들을 보면 한두 솔루션이나 서비스로 그 피해를 막기 힘들고 새로운 공격기법들이 속속 등장을 하고 있다. 이런 상황에서 모바일 환경을 제대로 보호하기 위해서는 결국 독립적인 한두 제품이 아닌 전체적인 보안 생태계 구축이 필요하며 이는 단순히 기술적인 것만이 아닌 입체적인 접근을 의미한다. 이에 모바일 보안 환경을 계선할 입체적인 생태계구축 방안에 대해서 논의할 필요성이 크다.

3. 연구의 목표와 내용

본 연구의 목표는 다음과 같이 정리될 수 있다. 첫째, 모바일 보안 산업/시장 동향 분석 및 전망을 한다. 건전한 모바일 산업 생태계를 구축하기 위해서는 모바일 보안산업이 태어난 배경과 현재 진행되고 있는 상황에 대한 자료 수집과 분석이 필요하다. 이를 바탕으로 앞으로 전개될 모바일 보안시장에 대한 예측해 본다. 이 예측은 국내 시장과 외국시장으로 나누어서 실시하되 외국 시장의 경우 앞으로 우리나라가 진출을 시도해 볼 가치가 크다고 판단되는 중국 시장에 대해서는 상대적으로 깊고 자세한 시장 분석을 한다.

둘째는 모바일 보안산업 경쟁력 육성 및 제고를 위한 핵심기술

R&D 및 기술 수요 실태조사·분석을 한다. 모바일 보안 시장과 산업은 그 속성상 범용 운영체제(Operating System)가 탑재된 스마트폰의 탄생이후 형성되고 있기 때문에 본격적인 모바일 보안시장의 탄생과 형성은 불과 2~3년전에 시작되었고 이제 태동기에 있다고 볼 수 있다. 따라서 모바일 보안 시장은 우리에게 특히 소프트웨어 기술과 시장에서 주도권과 경쟁력을 가지고 진출할 수 있는 좋은 기회이다. 이를 위해서는 먼저 모바일 보안산업에서의 핵심기술을 파악하고 이에 대한 연구개발을 선도적으로 시도해야 할 필요가 있다. 현실적으로 모바일 보안 핵심기술에 대한 연구개발 정보는 연구개발 주체뿐 아니라 보안산업 관련 종사자들에게 매우 민감하고 획득하기 어려운 관계로 이에 대한 실태조사와 분석은 한계를 가지고 있다.

셋째, 우라니라 모바일 보안산업에 관여하는 대기업, 중소기업, 소비자, 정부 등 시장의 각 주체들이 상호 발전을 하기 위한 모바일 보안시장 상생 프레임워크를 구축하는 방안에 대한 정책적 제언을 제공하는 것이다. 우리나라가 21세기 지구촌의 새로운 키워드인 디지털 융합과 유비쿼터스 사회에 있어서 핵심인 모바일 소프트웨어 플랫폼과 모바일 보안산업의 경쟁력을 확보하기 위해 국가적으로 어떤 전략을 택해야 하며 이러한 전략을 수행하기 위한 정부차원에서의 정책적 방안을 논의하는 것이 중요하다. 본 연구에서는 모바일 보안 시장을 소프트웨어 플랫폼 기반의 다면 플랫폼 시장으로 파악하고 관련된 산업 네트워크들이 서로 밀접하게 상호 작용하면서 하나의 생태계를 형성하여 진화해 산업이라는 공생적 프레임워크로 파악한다. 이렇게 어떤 플랫폼을 중심으로 관련 산업 네트워크가 밀접하게 상호작용하며 움직이는 산업 생태계가 국가적 차원의 경쟁력을 가지기 위해서는 무엇보다도 정부차원에서 지향해야 할 바른 방향의 지표들을 제시하고자 한다.

정리하면 본 연구에서는 다음 사항에 대한 연구를 수행한다.

- 모바일 보안 산업/시장 동향 분석 및 전망
  - 모바일 보안 정책 및 전략수립 지원을 위한 국내 모바일 보안 산업 현황 및 시장규모 분석

- 해외 주요국 모바일 보안 산업 현황 및 시장 규모 분석
- 해외 주요 모바일 보안기술 현황 조사 및 트랜드 분석

• 모바일 보안산업 경쟁력 육성 및 제고를 위한 핵심기술 R&D 및 기술 수요 실태조사·분석

• 대기업, 중소기업, 소비자, 정부 등 시장의 각 주체들이 상호 발전을 하기 위한 상생 프레임워크 구축 방안 마련

- 국내외 모바일 보안 산업 지원 정책의 비교 분석
- 모바일 보안 산업 육성 방안 마련
- 모바일 보안시장 확대 및 수출전략 등 전략적 육성 방안

제2장 모바일 보안산업 동향분석 및 전망

제1절 국내 모바일 보안산업 현황

1. 모바일 보안산업의 정의와 분류

(1) 보안산업의 정의와 분류

모바일 보안산업은 근본적으로 보안산업의 부분집합이기 때문에 먼저 보안산업에 대한 정의에서 출발해야 한다. 보안(Security)은 그 본질적인 성격상 물리 보안(Physical Security)과 정보 보안(Information Security)으로 나누어 질 수 있고 따라서 보안산업도 물리보안산업과 정보보안산업으로 나누어 질 수 있다. 그러나 20세기에 들어 정보통신기술의 혁신에 의한 정보화와 디지털화의 진전으로 두 산업간의 경계가 허물어지고, 특히 21세기에 들어 최근 물리적 보안과 IT기술 기반의 정보보안으로 양분화 되어 있는 영역자체가 융합되고 있는 추세이며, 이러한 융합의 중심에 있는 것이 융합보안이다. 융합보안은 과거 출입통제시스템, CCTV 등 개별적으로 운영·관리되어 왔던 물리적 보안영역과 IT보안시스템을 하나의 관리범위 안으로 통합함으로써 보안관리의 체계성을 확보하고 정보 유출 및 침해사고를 획기적으로 예방, 차단, 사후 추적 등이 가능하게 해준다.

우리나라에서 보안산업의 중요성을 깨닫고 이에 대한 비교적 명확한 정의와 체계적인 분류를 제공한 것은 2008년부터이다. 지식경제부는 ‘정보보안산업’ 및 ‘물리보안산업’, 그리고 ‘융합보안산업’이 결합된 산업군을 ‘지식정보보안산업'으로 명명하고 암호, 인증,

감시 등의 보안기술이 적용된 제품군을 생산하거나 관련 보안기술을 활용하여, 재난]재해.범죄등을 방지하는 서비스를 제공하는 산업으로 정의하였으며, 이에따라 『지식정보보안산업협회』를 중심으로 2001년부터 지식정보보안산업 통계조사를 실시하고 있다 [지식정보보안산업협회 2009, 2010].

정보보안통계조사의 연혁은 다음과 같다.

본 조사는 2001년「국내 정보보호산업 및 실태조사」로 최초 조사가 시행되었음

2004년「국내정보보호산업 통계조사」로 명칭을 변경함

2007년「국내정보보호산업 시장 및 동향조사」로 명칭을 변경하면서, 정보보호산업의 정책적 육성과제를 도출하고자 함

2009년「지식정보보안산업 시장 및 동향조사」로 명칭을 변경하면서 정보보호산업을 '정보보안산업, 물리보안산업, 융합보안산업'으로 확대하여 지식정보보안산업으로 전환함

2010년「국내 정보보안산업 실태 조사」로 정보보안산업에 대한 조사를 실시함

(2) 정보보안산업의 분류

정보보안산업의 분류는 정보보안산업의 특성상 제품과 서비스의 통합화 및 융합화가 매우 빠르게 진행되고 있어 정보보안산업을 분류할 때, 정보보안 하드웨어, 정보보안 소프트웨어, 정보보안 서비스의 3가지로 구분이 점차 모호해졌다. 이에 본 조사는 2006년, 2007년도 조사에서부터 델파이 기법을 이용하여 정보보안산업 관련 학계, 산업계 등 전문가로부터 산업품목에 대한 심도깊은 조사를 실시하여 자체적으로 정보보안산업 분류를 구성하였다.

정보보안 제품 및 서비스는 아래 <표 2-1>에서 보는 바와 같이 크게 '시스템 및 네트워크 정보보안 제품'과 '정보보안 서비스'의 두 부분으로 구분된다. 먼저, '시스템 및 네트워크 정보보안 제품'은 구체적으로 침입차단시스템, 침입방지시스템, 통합보안시스템, 보안관리, 가상사설망, 인증제품, 안티바이러스, 안티스팸, 보안운영체제,

통합 PC보안, DB/컨텐츠보안, 공개키기반구조, 접근관리, 기타 제품의 14가지로 분류할 수 있다. 둘째, '정보보안 서비스'는 세부적으로 유지보수, 보안컨설팅, 보안관제, 인증서비스, 기타서비스의 5가지로 구분하였다.

(3) 모바일 보안산업의 정의

『지식정보보안산업협회』의 정보보안산업분류(<표 2-1>)에 따르면 모바일 보안산업은 네트워크 보안 제품의 세부항목들중의 하나로 매우 협소하게 정의되어 분류되어 있음을 볼 수 있다. 모바일 보안산업을 이렇게 정의하면 통계조사 목적으로는 편리할지 모르지만 모바일 산업과 보안산업이 중첩되어 나타나는 모바일 보안 생태계에 대한 이해와 실제상황 파악에는 적합하지 않다. 그러면 과연 모바일 보안산업을 어떻게 정의해야 할까?

모바일 보안시장/산업에 대하여 현재까지 통일된 정의나 개념정립은 이루어지지 않고 있다. 그러나 2008년 아이폰의 등장으로 촉발된 스마트폰 혁명이후 글로벌 주요 IT Security 시장조사 기관들 – IDC, Frost & Sullivan, Juniper Networks Research, Infiniti Research Limited, Global Industry Analysts, Inc. 등 –은 전세계와 지역수준에서 모바일 보안시장에 대한 시장조사와 예측을 하고 있는데 이들에 의하면 모바일 보안시장/산업은 전통적인 유선 네트워크에 연결되는 PC와 고정 네트워크 기반시설(Fixed Network Infrastructure)에 발생하는 보안문제는 그 대상에서 제외하고 모바일 전화기, 스마트폰, 태블릿 PC, PDA, RFID, 무선센서 등 현대적인 의미의 모바일 기기에서 발생하는 보안문제를 해결하기 위한 소프트웨어/하드웨어 제품이라는 기본 개념을 공통분모로 하여 모바일 보안시장에 대한 시장조사와 시장예측을 위한 접근방법을 취하고 있다는 점에서 서로간에 모바일 보안시장에 대한 개념과 정의가 크게 다르지 않는 것으로 보여진다.

<표 2-1> 정보보안산업의 분류

대분류	소분류	기호	세부 항목
정보보안 제품	네트워크 보안	A	1 웹 방화벽 2 네트워크(시스템) 방화벽 3 침입방지시스템(IPS) 4 DDoS 차단 시스템 5 통합보안시스템(UTM) 6 가상사설망(VPN) 7 네트워크접근제어(NAC) 8 무선/모바일 보안
	시스템 보안	B	1 PC 방화벽 2 Virus 백신 3 Anti 스파이웨어 4 Anti 피싱 5 스팸차단 S/W 6 보안운영체제
	컨텐츠/ 정보유출 방지보안	C	1 DB보안 2 DB암호 3 PC보안 4 보안 USB 5 디지털저작권관리(DRM)
	암호/인증	D	1 보안스마트카드 2 H/W토큰(HSM) 3 일회용비밀번호(OTP) 4 공개키기반구조(PKI) 5 통합접근관리(EAM) 6 싱글사인온(SSO) 7 통합계정관리(IM/IAM) 8 공인/사설 인증 툴
	보안관리	E	1 기업보안관리(ESM) 2 위협관리시스템(TMS) 3 패치관리시스템(PMS) 4 자산관리시스템(RMS) 5 로그 관리/분석 툴 6 취약점 분석 툴
	기타 제품	F	1 기타

<표 2-1> (계속)

대분류	소분류	기호	세부 항목
정보보안 서비스	보안컨설팅	G	1 인증(ISO, ISMS) 2 안전진단/기반보호 3 진단 및 모의해킹 4 개인정보보호 5 종합보안컨설팅
	유지보수	H	1 판매 후 유료서비스
	보안관제	I	1 보안관제 서비스
	교육/훈련	J	1 교육훈련 서비스
	인증서비스	K	1 공인/사설 인증서비스

예를 들어 대표적인 시장조사기관인 IDC에 따르면 2015년 전 세계 모바일 보안시장은 190억 달러 규모로 2010년의 4억700만 달러에서 비약적인 성장을 기록할 것으로 전망하고 있고, 이 예측치는 모바일 보안 소프트웨어 제품들을 다음과 같이 분류하고 있다.

- Mobile IPC (Information Protection and Control): DLP (Data Loss Prevention)와 Encryption을 포함
- MIAM (Mobile Identity and Access Management)
- MSVM (Mobile Security and Vulnerability Management)
- Mobile Threat Management,
- Mobile VPN(Virtual Private Network)
- MOS(Mobile Operation Security)

IDC는 이러한 제품군들의 매출액이 2010년부터 2015년 사이에 연간 평균 30% 이상의 성장률을 보일 것으로 예측되었다. 아래 표 <2-2>는 IDC가 매출액 기준으로 예측한 전세계 모바일 보안 시장규모와 성장 추이를 보여주고 있다.

<표 2-2> 전세계 모바일 보안시장 예측

Mobile Security Product Sales Forecast(Million USD)

	2010	2011	2012	2013	2014	2015	2010–2015 CAGR (%)
Mobile threat management	99.1	179.2	280.2	350.1	415.2	470.4	36.5
Mobile IPC (encryption + DLP)	78.2	140.1	238.3	334.9	405.1	460.2	42.5
Mobile VPN	125.2	190.2	259.6	330.1	385.2	431.2	28.1
MIAM	43.8	69.9	117.1	164.2	194.8	225.7	38.8
MSVM	40.2	65.7	94.8	129.1	160.5	190.2	36.5
MOS	20.4	29.7	44.1	53.9	64.9	75.1	29.8
Total	406.9	674.8	1,034.10	1,362.30	1,625.70	1,852.80	35.4

Source: International Data Corporation(IDC)

2. 우리나라 모바일 보안산업 현황

한국인터넷진흥원이 24일 발표한 2010년 정보보안 시장 조사 결과, 정보보안 시장이 1조원을 넘어선 것으로 나타났다. 분야별로는 웹방화벽, 디도스 차단 시스템, 통합보안시스템 등이 포함된 네트워크보안 분야가 3천246억원으로 가장 많은 비중을 차지했다. 또한 DB보안과 PC보안, DRM 등이 포함된 콘텐츠·정보유출방지보안 분야가 1천812억원으로 그 뒤를 이었고 바이러스백신과 보안운영체제, 안티스파이웨어 등 시스템보안(1천434억원)과 기업보안관리, 위협관리시스템 등 보안관리(1천91억원) 등도 큰 비중을 차지했다. 눈에 띄는 부분은 지난해 매출 증가율이 가장 높았던 무선·모바일 보안 분야다. 스마트폰과 태블릿PC 보급으로 시장이 급격히 성장해 2009년 대비 79.3% 성장한 266억원을 기록했기 때문이다. 이밖에 네트워크접근제어(NAC)는 58.6%, 통합보안시스템(UTM)은 47.4%, 디도스 차단시스템은 44.5% 성장하는 등 2009년 대비 높은 증가율을 보였다.

지난해 국내 정보보안산업이 총 매출액 1조원을 넘어섰다. 지난해 로봇 산업도 2009년 기준으로 1조원 시장에 진입하면서 이목을 끌었는데, 2000년대 초 IT 열풍과 더불어 시장을 키워나간 국내 정보보안 시장이 어느덧 10년을 넘어 1조원 시장까지 돌파했다. 한국인터넷진흥원과 지식정보보안산업협회가 함께 국내 정보보안 114개 사업체를 대상으로 실시한 '2010년 국내 정보보안산업 실태조사'보고서를 통해 국내 정보보안시장 현황을 살펴보면 다음과 같다.

[그림 2-1] 2010년 우리나라 정보보안 분야별 매출액

이번조사에 따르면 지난해 국내 정보보안시장은 2009년 대비 21.6% 성장한 1조 1300억원을 기록했다. 이중 정보보안 제품부문은 전년 대비 21.1% 성장한 9168억원, 정보보안 서비스 부문은 23.8% 증가한 2146억원으로 각각 집계됐다. 분야별로는 웹방화벽, 분산서비스거부(DDoS)차단시스템 등 네트워크 보안 분야가 3246억원으로 가장 많은 비중을 차지했다. 이어 데이터베이스보안, PC보안 등 컨텐츠 및 정보유출방지 보안분야가 1812억원, 바이러스 백신, 보안운영체제, 안티스파이웨어 등 시스템 보안이 1434억원, 기업보안관리, 위협관리시

스템 등 보안관리가 1091억원으로 뒤를 이었다.

매출 증가율이 가장 높았던 분야는 무선·모바일 보안으로 전년 대비 79.3% 성장한 266억원을 기록했다. 특히 무선·모바일 보안 솔루션은 금융(31.3%)과 공공(29.5%) 분야에서 수요가 많았고 교육(13.6%)과 대기업(13.5%)도 일정부분 수요가 있는 것으로 나타났다. 보고서는 무선·모바일보안의 경우 아직 시장 규모는 크지 않지만 최근 스마트폰, 태블릿PC 등의 보급으로 인해 관련 업계에서는 다양한 보안솔루션을 개발하는 등 시장 규모가 급증하는 추세라고 분석했다.

국내 정보보안시장은 2015년까지 연평균 6.6% 내외의 지속적인 성장률을 보여, 오는 2015년경 1조 5000억원 이상의 시장으로 확대될 것으로 예상했다. 이중에서도 분산 서비스거부(DDoS) 차단 시스템 분야가 연평균 14.9% 성장률을 보이며 오는 2015년경 549억원 규모의 시장을 형성할 것으로 예측됐다. 보고서는 DDoS 차단시스템이 2007년부터 매출액이 조사된 비교적 최신 제품임에도 불구하고, 과거 연평균 성장률이 95%에 달했으며, 앞으로도 높은 성장이 예상되는 시장이라고 전망했다.

또 무선·모바일 보안 시장도 연평균 13.7%의 성장률을 보이며 2015년경 506억원대의 시장을 형성할 것으로 조사됐다. 특히 이 시장은 최근 스마트폰과 아이패드 등의 열풍으로 인해 큰 성장을 이를 수 있을 것으로 예상됐다. 이밖에도 안전진단 컨설팅, 보안USB, 디지털 저작권 관리(DRM ㅋ)시장이 각각 17.8%, 14.9%, 14.2%의 성장률을 보일 것으로 나타났다. 반면, 일회용 비밀번호(OTP) 분야는 연평균 26.8 %의 하락율을 보여 2015년엔 지난해 대비 (9억5300만원) 7억원 가까이 하락한 2억원대 시장을 형성할 것으로 분석됐다. PC 방화벽 매출도 연평균 23.3% 하락, 2015년경에는 지난 해 27억원보다 20억원 가량 줄어든 7억원 규모의 시장을 형성할 것으로 전망되었는데. 액티브 X 기술을 활용한 인터넷 보안 기능 강화로 꾸준히 성장해 왔지만, 액티브 X기술을 채택하는 곳이 줄어들 것으로 예상됨에 따라 시장도 축소될 것으로 보고서는 분석했다. 이밖에도 패치관리시스템과 기업보안관리시장이 각각 9%, 7.3% 하락율을 보일것으로 보고서는 전망했다.

[그림 2-2] 2010년 우리나라 모바일보안 기관별 매출액

지난해 수출액 21% 증가된 것으로 나타났으며, 최대 수출국은 일본이었다. 지난해 국내 정보보안 제품 수출은 전년 대비 약 21.6% 증가한 520억원을 기록했다. 사업체 매출액 기준으로는, 매출액 90억원 이상의 사업자들이 전체수출의 73.5%를 차지하고 있는 것으로 나타났다. 기업형태별로는 벤처기업이 전체 수출의 79%인 411억 9300만원을 수출하고 있으며 나머지 20% 가량을 일반기업이 담당하고 있어 벤처기업들이 수출을 주도하고 있는 것으로 나타났다. 우리나라 정보보안 제품의 최대 수출국은 이웃 국가인 일본으로 나타났는데. 전체 수출의 약 69.32%가 일본이고 기타 국가 12.6%를 제외하고 미국 9.3%, 중국 7.8% 순으로 집계됐다. 보고서는 일본 비중이 큰 반면, 중국은 7.8%에 불과하다며 향후 중국의 정보보안 산업이 발전할 것을 감안, 국내 기술경쟁력을 향상시켜 수출 경쟁력을 높일 필요가 있다고 덧붙였다.

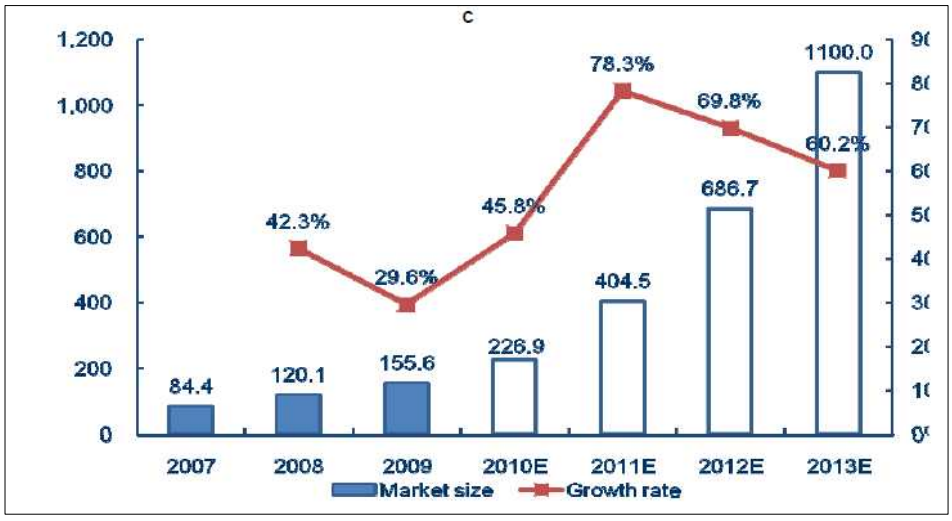
제2절 중국의 모바일 보안산업 현황

1. 중국의 무선 인터넷 시장 애플리케이션 현황 분석

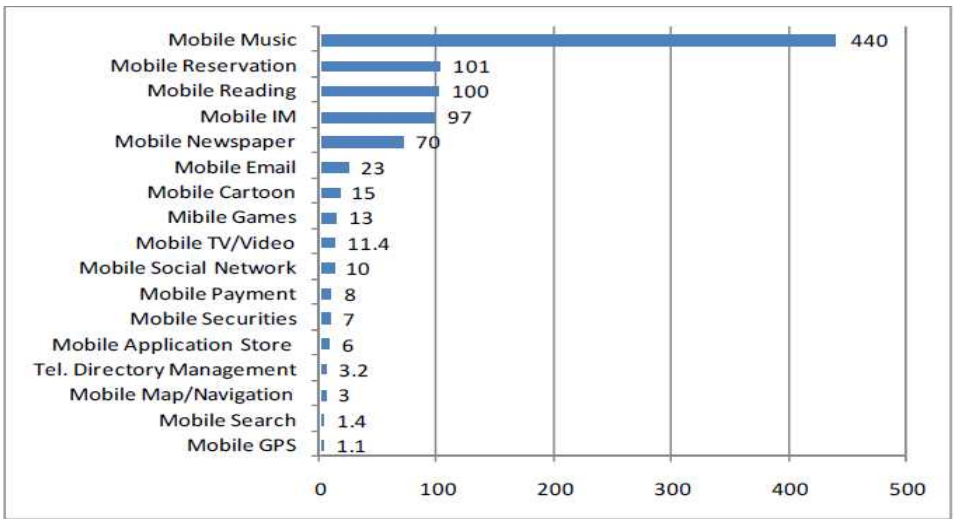
(1) 무선 인터넷 시장 현황 개요

10년 전 무선 인터넷이 처음 등장한 이래 시장규모는 연 30% 이상의 성장률을 보이며 계속해서 확대를 거듭해왔다. 2009년 말 중국의 무선 인터넷 시장규모는 약 2천억위안까지 근접했다. 무선 인터넷의 발전은 업무와 일상 모두에서 급증하는 정보 수요를 충족시켰음은 물론, 거대한 신규 산업사슬을 형성했다. 유무선 인터넷 통합의 결과로 2010년부터 2013년까지 모바일 QQ와 같은 회원제 모바일 인터넷 서비스가 인터넷 산업 전체 수익에서 차지하는 비중은 더욱 늘어날 것으로 예상된다. 게다가 단말기 시장에 대거 유입되고 있는 스마트폰의 수를 감안하면 무선인터넷 시장의 규모는 성장세를 이어갈 것으로 보인다.

[그림 2-3] 중국의 무선인터넷 시장성장 전망

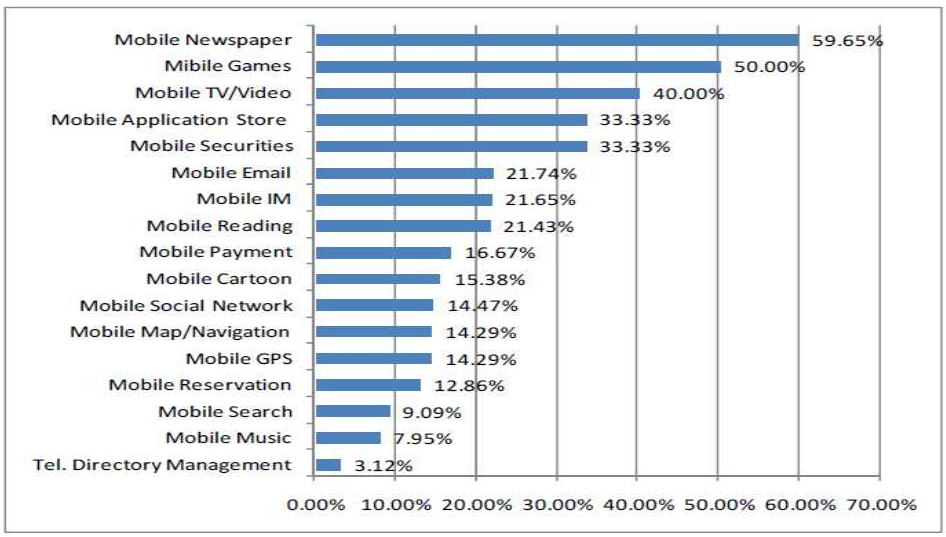


[그림 2-4] 중국 모바일 앱 사용자 수(2010년 단위 백만)



3G 통신망의 보급화와 갈수록 점증하는 스마트폰의 시장점유율에 힘입어 음악, e-리더, 게임, 메신저, 이메일, TV, 증권, 커뮤니티, 여행정보, 사진출력, SMS 관리, 만화 등 모바일 애플리케이션의 종류와 양은 가파르게 증가하고 있다.

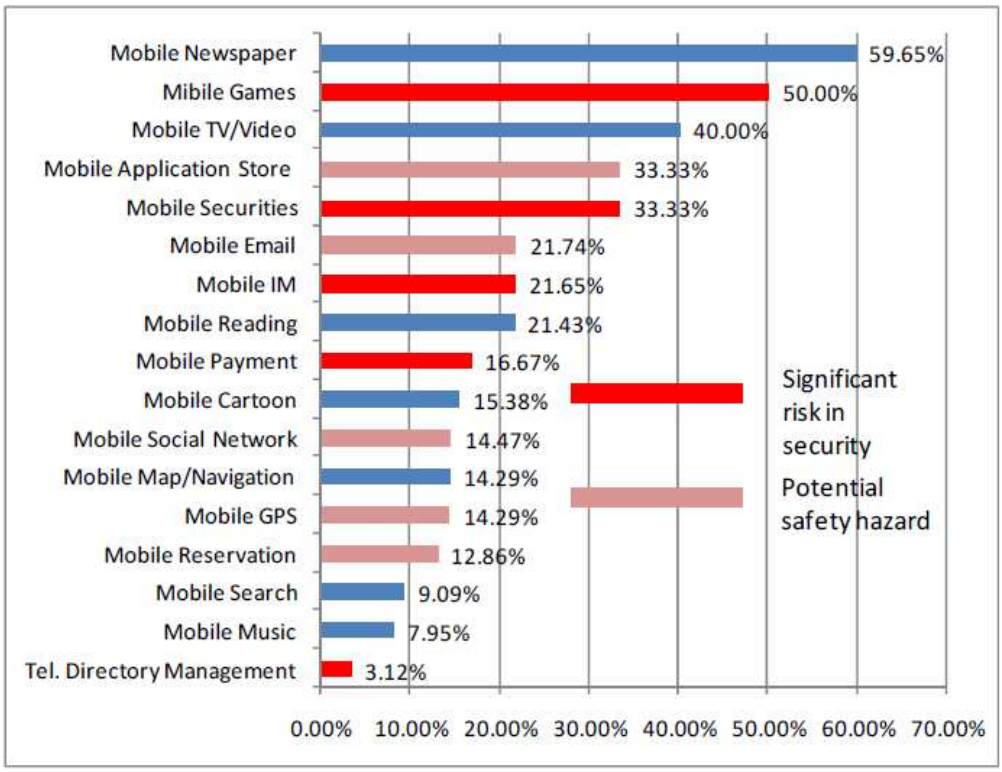
[그림 2-5] 모바일 앱사용자수 증가율



위 그림([그림 2-3])을 보면 신문, 게임, TV, 증권 등의 모바일 앱이 가장 많은 사용자층을 확보하고 있음을 알 수 있다. 또 [그림 2-5]에서 보듯 모바일 애플리케이션 (이하 앱) 사용자수는 2010년 한해 빠르게 성장했다.

대부분의 사용자들에게 있어 특정 모바일 앱을 선택하는 핵심동기는 실용성으로, 보안 문제는 주요 관심영역에서 벗어나있다. 그러나 모바일 앱의 대중화가 진행될수록 보안 관련 문제는 갈수록 대두될 것이다. 최근 통계에 따르면 하단 그림([그림 2-6])에 드러나 있듯 10가지 유형의 앱 서비스에 잠재적 위험요소가 존재하고 있으며, 이 가운데 5개 유형은 심각한 보안문제를 안고 있다. 게임, 증권거래, IM, 전자결제 및 전화번호부 관리 등 5개 분야 모바일 앱은 심각한 수준의 보안문제를 안고 있다.

[그림 2-6] 모바일 앱 분야별 성장률과 보안문제 수준

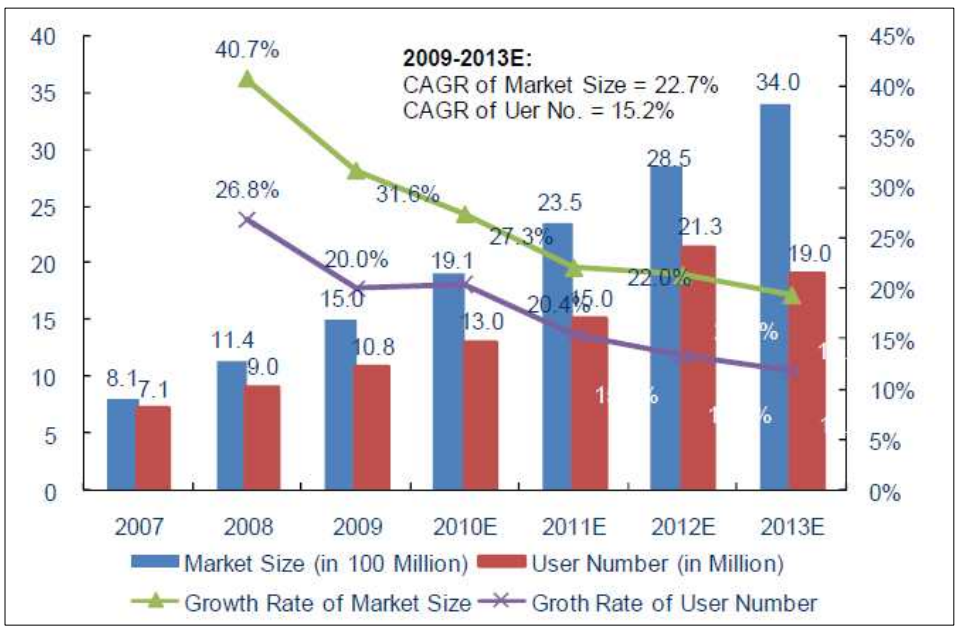


(2) 모바일 앱 및 보안 수요 분석

① 모바일 게임 보안 수요

중국 내 모바일 게임 시장규모는 2009년 기준 15억위안에 도달했으며, 이는 2008년에 비해 31.6%나 성장한 수치다. 모바일 게임 시장의 주된 수입원은 단독형 (오프라인) 모바일 게임이며, 온라인 모바일 게임은 작은 비중만을 차지하고 있다. 다만 스마트폰과 3G 서비스가 대중화 추세에 있으므로 향후에는 온라인 모바일 게임이 모바일 게임 시장 전반을 잠식할 것으로 예상된다. 또한 온라인 게임의 가입자평균매출(ARPU)이 매우 높음을 감안하면 계속해서 다수의 콘텐츠 제공자(CP)와 서비스 제공자(SP)가 시장에 참여할 것으로 보인다. 모바일 게임 시장은 새로운 성장을 견인할 것으로 기대되며, 총 시장규모는 약 28억 5천위안에 달할 것으로 전망된다. 벤처투자자(VC)들도 모바일 온라인 게임 시장의 급속한 성장에 주목하기 시작했다.

[그림 2-7] 모바일 게임시장 성장 전망

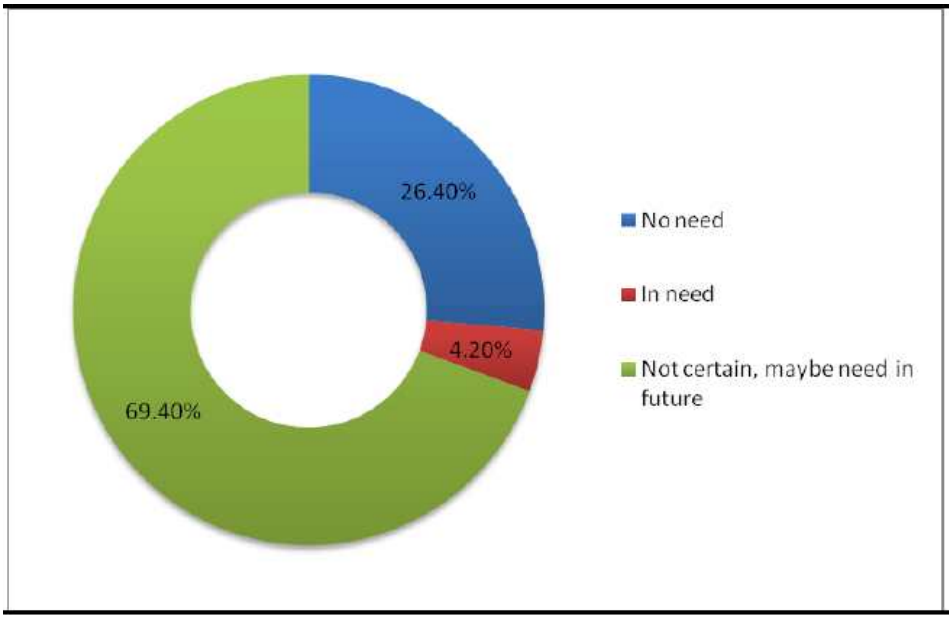


모바일 게임업계 가치사슬의 3대 대표주자는 통신사업자, Tencent, 그리고 단말기 제조사이며, 과금 채널과 사용자를 보유한 통신사가 업계 전체를 주도하는 한 축이다. 한편 Tencent도 사용자수와 성숙한 과금체계를 이용해 시장점유율을 높여가며 통신사들을 위협하고 있다. 또한 애플과 같은 단말기 제조사도 사용자층에 큰 영향력을 발휘하며 시장점유율 상향을 위해 온라인 앱스토어를 구축하고 있다.

<표 2-3> 모바일 온라인게임에 대한 벤쳐캐피탈 투자

Company	Industry	Investment amount	Investor	Time
SOCO SOFT	Mobile Games	20 Million	Green Pine Capital	2009-11-5
Showina Digital Technology	Mobile Games	2 Million	Yonghui Ruijin Venture Capital	2009-8-21

[그림 2-8] 모바일 게이머들의 보안의식



온라인 게임은 컴퓨터 및 휴대전화에서 바이러스 감염을 일으키는 주범 가운데 하나다. 온라인 게임은 타임 카드와 아이템을 이용해 요

금을 부과하나, 모바일 온라인 게임에서는 후자가 더 많이 이용된다. 따라서 게임 아이템은 자연히 사용자들의 계정 정보를 훔치려는 해커들과 바이러스의 목표가 되고 있음에도 대다수의 모바일 온라인 게임 사용자들은 보안에 거의 무관심하다. 휴대전화를 대상으로 하는 바이러스는 모바일 온라인 게임과 보조를 맞추어 더욱 늘어날 것이며, 사용자와 통신사 모두에게 더 큰 위협으로 작용할 것이다. 그러므로 온라인 게임용 보안 분야는 모바일 통신기기 보안에 있어 주요한 향후 흐름 중 하나로 자리잡을 것이다.

가장 최근의 설문 결과를 보면 모바일 온라인 게임에 '보안이 필요하지 않다'고 응답한 사람은 전체의 26.4%에 불과했다. 모바일 온라인 게임산업의 성장세를 감안하면 단 한 편의 게임일지라도 휴대전화 보안의 필요성을 제고시키는 계기가 될 수 있을 것이다.

② 모바일 증권거래 보안 수요

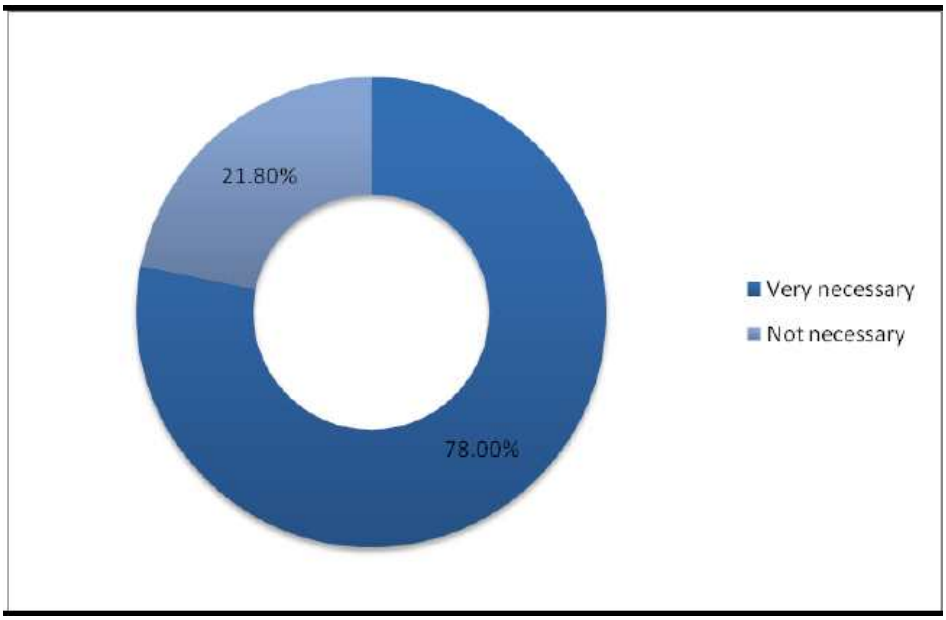
중국 증시는 5년간의 침체기 이후 2006년을 기점으로 급속한 성장세를 보여왔다. 2007년 1월 9일 기준으로 중국 증시의 시가총액은 10억위안에 도달했다. 골드만 삭스의 Frederick Zuliu Hu 아시아 담당 상무이사는 중국 증시 시가총액이 향후 1조위안을 돌파해 시장규모 면에서 세계 3위로 자리매김할 것으로 예상한 바 있다.

대부분의 직장인 주식투자자들은 직접 거래소를 찾을 시간적 여유도 없을뿐더러 업무시간 중 주식거래는 금지된 경우가 많다. 사무실에서 PC나 전화를 이용한 주식거래도 여의치 않다 보니 모바일 증권거래를 이용하게 되는 것이다. 모바일 증권거래 앱은 기존의 온라인 증시분석 시스템과 휴대전화를 함께 활용해 인터넷 및 이동통신망 기반의 증권거래 플랫폼과 모바일 클라이언트, WAP, SMS, USSD 등을 이용한 금융 부가가치 서비스를 제공한다. 또한 주식시장의 움직임을 실시간으로 파악할 수 있는 효과적인 도구가 필요한 대부분의 개인투자자들에게도 휴대전화가 각광받고 있다.

중국 내 모바일 증권거래 서비스는 새로운 것이 아니다. 2003년

초 China Mobile, China Unit, Nokia, Handinweb을 비롯한 몇몇 업체가 이미 해당 서비스를 출시한 바 있으나, 증시 난조로 인해 그다지 성공을 거두지는 못했다. 그러나 2006년 이후, 특히 2007년을 기점으로 증시가 활황세로 돌아섬과 함께 통신사와 SP, 독립 콘텐츠 제공자 및 소프트웨어 제조사들의 적극적인 홍보가 이어지며 모바일 증권거래 서비스는 업계 제반 환경과 사용자수 모두에 있어 괄목할만한 성공을 이루었다. 2010년 말 기준으로 모바일 증권거래 (모바일 클라이언트 포함) 사용자수는 1백만명을 넘어섰다.

[그림 2-9] 모바일 증권투자자들의 보안의식



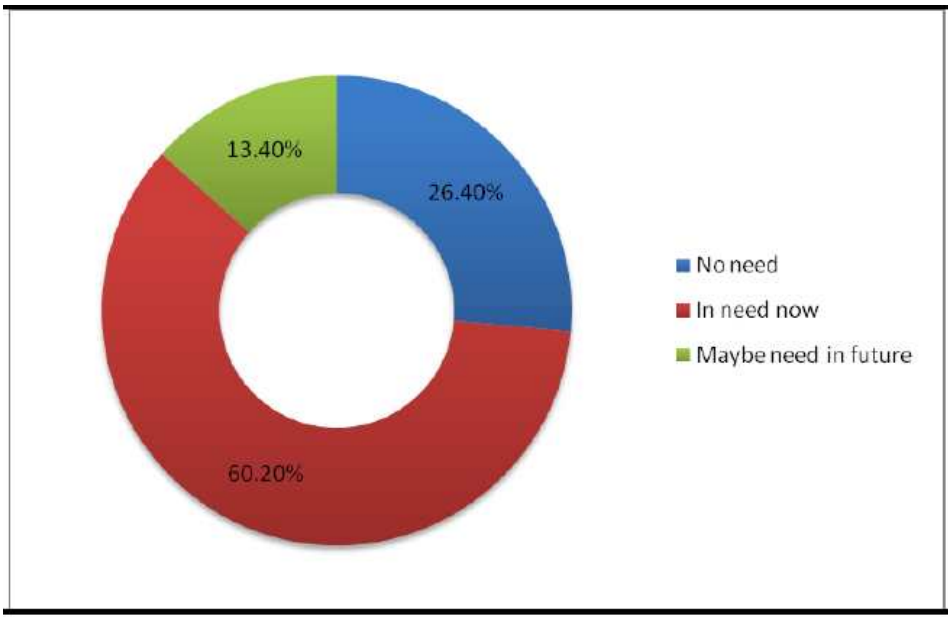
사실 3, 4년 전 일부 증권사 역시 모바일 증권거래 서비스를 개시한 바 있으나, 기술적 완성도_및_비즈니스 모델 측면에서 취약함을 보이며 다수의 사용자에게 어필하는 데는 실패했다. 오히려 과금정책의 빈번한 변경과 소프트웨어 및 제공 정보의 느린 업데이트, 모바일 클라이언트의 불편한 체감성능 등 다양한 요인으로 인해 다수의 고객이 이탈했다.

모바일 증권거래 앱은 시장점유율이 여전히 작기 때문에 아직 바이러스의 공격 목표가 되고 있지는 않다. 하지만 개인 금융계좌와 직접적으로 연결되어있다는 점에서 보안은 여전히 사용자들의 주된 관심사이며, 향후 보안 소프트웨어에 대한 필요성이 증대될 것으로 예상할 수 있다.

③ 모바일 IM 보안 수요

모바일 인스턴트 메시징(IM)은 중국 내 모든 모바일 앱을 선도하는 성장점으로 자리잡았다. 2007년 이후 중국 내 모바일 IM 시장은 사용자수와 시장규모 모두에서 PC용 IM과 기업용 IM 시장보다 빠른 속도로 성장해왔다. 모바일 IM 시장은 유무선 인터넷의 통합이 주도한 다양화 추세를 그대로 따르고 있으며, 스마트폰과 3G 통신망의 대중화가 진행되면서 모바일 IM의 사용은 더욱 더 보편화되고 있다. 2010년 말을 기준으로 모바일 IM 총 사용자수는 4억 1천만명에 육박하고 있으며, 이 가운데 실사용자(active user)는 1억 9천만명에 달한다.

[그림 2-10] 모바일 IM 사용자들의 보안의식



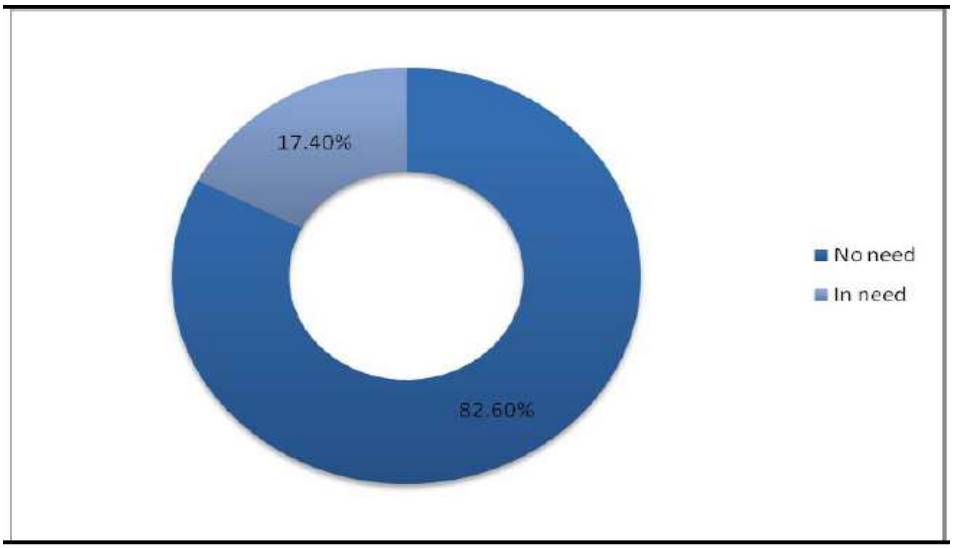
모바일 IM 실사용자 시장은 그다지 변수가 없는 상황에서 모바일 QQ가 52.1%의 시장점유율을 보이며 1위를 지키고 있으며, 그 뒤를 모바일 Fetion과 모바일 MSN이 잇고 있다.

악성코드는 PC 기반 IM 소프트웨어와 나란히 늘어나고 있으나, 대부분의 보안 백신으로 탐지 및 치료가 가능한 상황이다. 또한 현재는 대부분의 주요 IM이 모바일 버전도 함께 제공하며 점점 더 많은 사용자들이 모바일 클라이언트를 이용해 접속하고 있다. 효과적인 관리가 이루어지지 않는다면 모바일 IM만을 노리는 악성코드가 더욱 기승을 부릴 것으로 전망된다.

④ 모바일 결제 보안 수요

윈도우 쇼핑에서 온라인 쇼핑, 그리고 오늘날의 모바일 쇼핑에 이르기까지 소비자들의 쇼핑 수단은 3G 통신망과 전자상거래 관련기술의 발달과 함께 일대 변혁을 겪어왔다. 그 결과 소비자들은 더욱 간편하게 쇼핑을 즐기게 되었을 뿐 아니라 서비스 수준의 질적 향상과 함께 가격 인하 혜택까지 누리게 되었다.

[그림 2-11] 모바일 결제 사용자들의 보안의식



2009년 기준 중국 내 온라인 금융결제 총액은 2천 586억위안에 달했으며 2006년 312억위안, 2007년 594억위안에 이어 연간 105.8%에 이르는 성장률을 보였다. 온라인 쇼핑의 대중화 속도는 계속 빨라지고 있으며, 이는 모바일 쇼핑이 제공하는 편의성에 따라 더욱 가속화 될 것으로 보인다.

모바일 결제는 모바일 쇼핑의 핵심이며, 이동통신사 가운데 유일하게 China Mobile만이 시장규모 수치가 존재하지 않던 2010년 2월부터 모바일 결제 서비스 홍보를 시작했다. 현 추세라면 모바일 쇼핑 총액은 2010년 말까지 11억 5천만위안에, 2013년까지는 70억위안에 도달할 것으로 예상된다. 통신사가 제공하는 모바일 결제 서비스는 주로 전화요금 납부 수단으로 사용되고 있으며, 현재 총 금융거래의 90% 이상을 차지하고 있다. 최근에는 Taobao 사용자들의 계정 정보를 무단 갈취하는 'Kidnapping Taobao' 트로이 목마 바이러스가 위세를 떨치고 있는데, 향후 모바일 결제 서비스의 증가 역시 필히 모바일 보안에 대한 수요를 견인할 것으로 보인다.

⑤ 전화번호부 관리 보안 수요

전화번호부는 휴대전화 사용자들에게 매우 중요한 데이터에 해당하며, 해킹에 의해 유출될 경우 자신도 모르는 사이 주변 인물들에게 광고 또는 허위 메시지를 전송하는 데 악용될 수 있다. 프로스트&설리번의 조사에 의하면 전화번호부에 대한 핵심 보안수요는 다음과 같다:

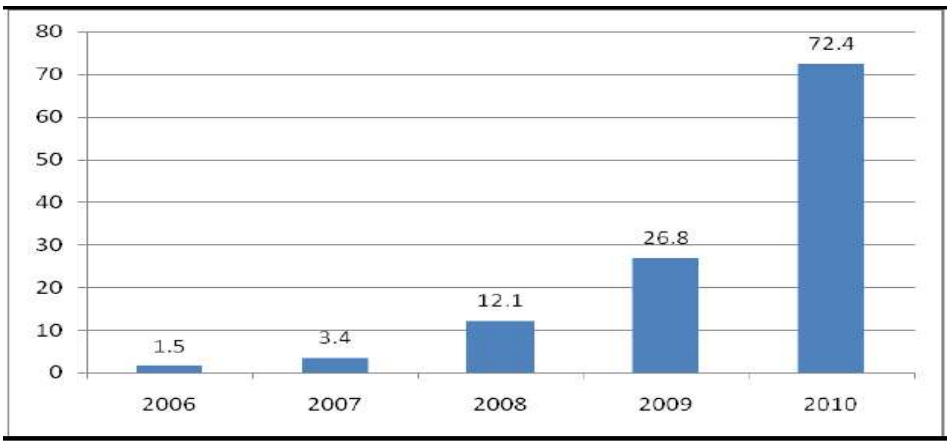
1. 기기 변경 시 새로운 전화기로의 전화번호부 데이터 백업 및 복원
2. 연락처 정보의 암호화 또는 보안설정을 통한 전화번호부 무단취득 방지
3. 악성코드나 바이러스에 의한 전화번호부 유출 방지
4. 전화번호부 유실에 의한 개인정보 도난 방지를 목적으로 하는 원격 잠금 설정

2. 중국 내 모바일 보안시장 개관

(1) 중국 모바일 보안제품 시장 규모

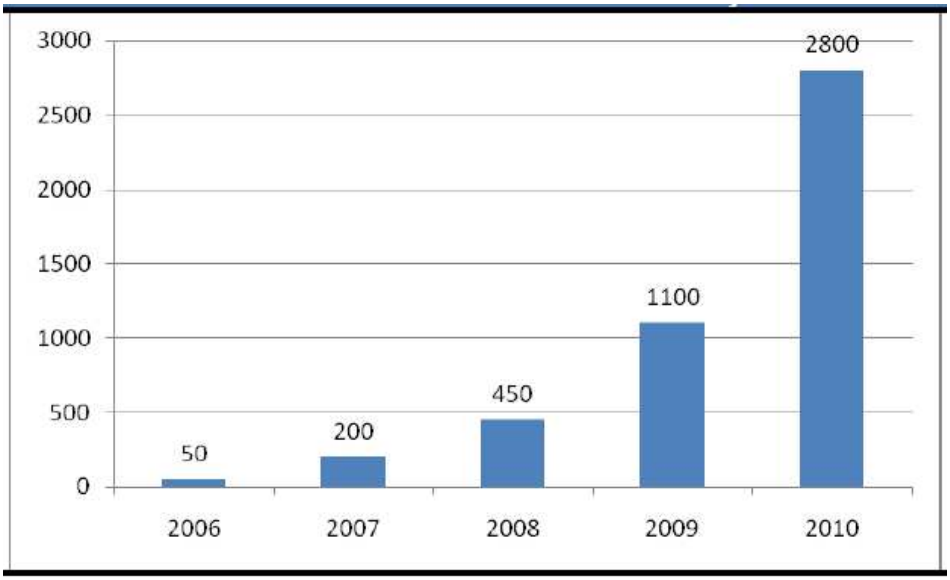
2010년 들어 모바일 보안 관련 사건사고는 전년도에 비해 더욱 증가했고 그 폐해 또한 심각해졌다. 그 결과 소비자들은 모바일 보안문제의 심각성에 대해 깨닫게 되었고, 통신사와 단말기 제조사들 역시 보안 문제를 주요사안으로 취급하며 협력하기 시작했다. 스마트폰 사용자가 급속도로 증가하고 있는 상황에서, 위와 같은 조건들이 하나로 수렴되며 모바일 보안제품 시장도 빠르게 덩치가 커져가고 있다.

[그림 2-12] 중국내 모바일 보안제품 활성 사용자(Activated Users)수의 성장추세 (단위 백만)



2010년 6월 말을 기준으로 중국 내 모바일 보안제품 활성 사용자 수는 5천 4백만명에 도달했으며, 실사용자 수는 2천 4백만에 달해 2009년 동기 대비 100% 증가한 수치를 기록했다. ([그림 2-12]와 [그림 2-13] 참고)

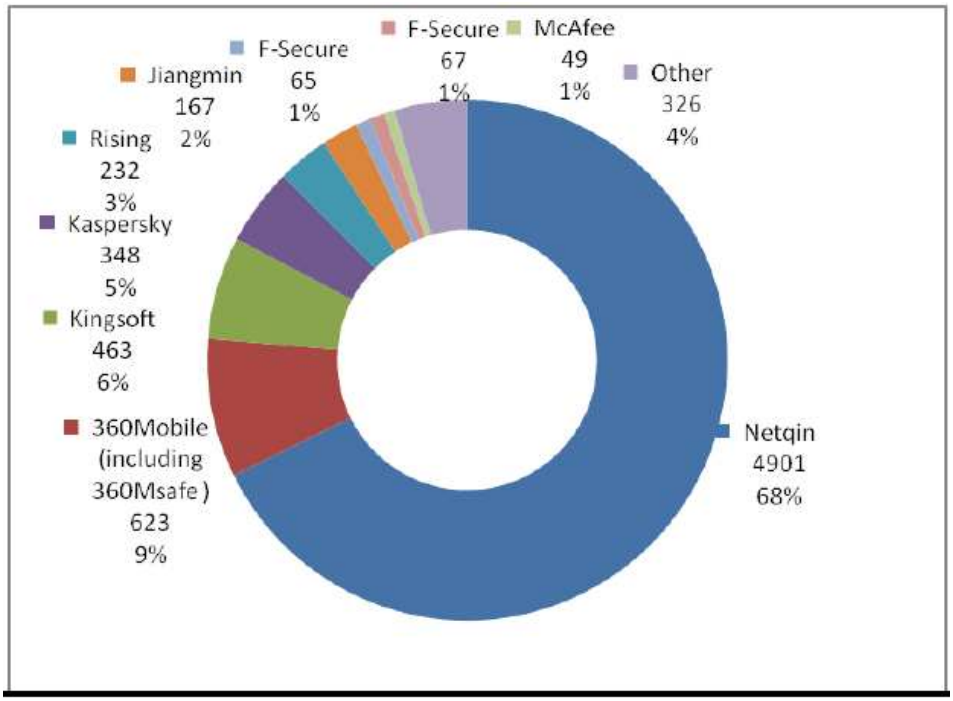
[그림 2-13] 중국내 모바일 보안제품 실사용자수의 성장추세 (단위 백만)



(2) 중국 모바일 보안업체 시장점유율

2010년 말을 기준으로 중국 내 모바일 보안제품의 활성 사용자수는 7천 240만명을 기록했다. 활성 사용자수로 시장점유율을 파악해보면 NetQin의 활성 사용자수가 4천 9백만명으로 67.7%의 시장점유율을 보였다. 360 Mobile과 Kingsoft Mobile의 경우 공격적인 체험 마케팅을 펼친 결과 시장점유율을 빠른 속도로 높일 수 있었다. 양사의 활성 사용자수는 각각 620만명, 460만명으로 집계됐다. Kaspersky의 경우 무료 제품들이 유료 제품군의 시장점유율에 악영향을 미친 것으로 나타났다. 기타 보안용 무료 SW를 선호하는 사용자가 꾸준히 늘어나고 있는 상황이며, 프로스트&설리번은 F-Secure, Symantec, McAfee와 같이 중국에 진출한 해외 보안업체들의 시장점유율이 각 1%를 넘지 않는 것으로 추정하고 있다.

[그림 2-14] 중국내 모바일 보안제품별 활성사용자의 점유율



(3) 중국 내 주요 모바일 보안업체 GEM(Growth Excellence Matrix) 분석

중국 모바일 보안시장은 현재 도입단계에 있으나 폭발적인 시장 잠재력을 보유하고 있다. 향후 2, 3년 내 해당 시장은 고속 성장단계에 진입할 것으로 예상되므로, 기업의 성장역량에 대해 주목하지 않을 수 없다. 높은 성장력을 갖춘 기업은 시장의 고속 성장기에 더 높은 시장점유율을 확보함은 물론 경쟁방식 자체를 변화시킬 수 있을 것이다.

<표 2-4> Growth Strategy Excellence Evaluation of Major Security Vendors

	NetQin	360 Mobile	Kingsoft	Kaspersky	360 Msafe	Rising	Jiangmin	F-Secure	Symantec	McAfee
1. Growth compared to industry growth	9	8	7	8	8	7	6	4	4	4
2. Growth compared to fastest growing competitor	10	9	6	6	7	6	3	3	2	4
3. Global perspective of strategy	9	8	7	8	6	6	4	10	10	10
4. Integration of Competitive Positioning/Branding	10	8	8	9	7	9	7	5	7	6
5. Integration of Customer Analysis	9	10	8	7	8	6	4	6	5	5
6. 360 Degree Analysis (TEAM)	8	7	7	8	7	6	4	8	7	6
7. Integration of industry challenges, drivers, restraints, trends	9	7	8	10	5	9	9	9	8	9
8. A growth system or growth pipeline	9	8	7	7	8	6	5	7	7	8
9. Visionary leadership	9	8	7	9	8	6	8	7	6	7
10. Management team integration (Growth Workshops)	9	10	9	6	7	8	7	5	6	6

프로스트&설리번의 GEM 조사방식은 성장전략 우수성(<표 2-4>)과 실행능력 우수성(<표 2-5>)의 두 측면 모두에 평점을 부여해 비교 대조함으로써 제조업체의 성장역량을 평가하며, 각 제조사의 성장역량을 GEM 조견표 상에 표시해 보여준다.

<표 2-5> Implenentation Excellence Evaluation of Major Security Vendors

	NetQin	360 Mobile	Kingsoft	Kaspersky	360 Msafe	Rising	Jiangmin	F-Secure	Symantec	McAfee
1. Team consensus on Growth Strategy	9	8	8	7	8	7	5	7	6	5
2. Best Practices for Marketing/Business Development	10	10	9	8	9	6	4	6	6	7
3. Best Practices for Sales	9	10	3	4	9	5	2	3	4	4
4. Best Practices for Management & Leadership	9	6	8	8	7	7	7	8	8	8
5. Sense of Urgency	8	8	8	6	8	6	8	5	5	5
6. Implementation Training Process	10	6	9	9	7	8	6	4	5	6
7. Implementation Discipline	9	8	8	7	8	8	7	6	5	5
8. The Growth Environment	10	7	8	8	8	7	6	4	3	4
9. Internal Resistance: NIH, Corporate Antibodies, etc.	6	5	5	4	5	5	6	6	6	5
10. Strength of Management Team to Drive Change	9	8	8	6	8	7	6	5	5	4

프로스트&설리번은 주요 제조사에 대한 성장전략 및 실행능력 복합 평가 결과를 중국 내 모바일 보안업체에 대한 GEM 조견표로 잘 보여주고 있으며([그림 2-15]), 해당 결과에 따르면 NetQin이 두 항목 모두에서 최우수 평점을 받았고 360과 KingSoft, Kaspersky가 순서대로 그 뒤를 이었다.

[그림 2-15] GEM Matrix of Major Security Vendors

<표 2-6> The Analysis on Competitive Advantages and Dsiadvantages of Major Vendors

	Competitive Advantages	Competitive Disadvantages
NetQin	1. Broad product lines with perfect functions 2. Strong ability in market promotion and multiple channel development 3. Stable SaaS business model 4. Greater investment in R&D with multiple technical patents 5. Supporting various smartphone systems with stronger adaptation 6. Perfected after-sales service and dedicated customer service team 7. Committed to mobile security, earlier entrance in market with first - mover advantage 8. Global market development capability with 51.5 million accumulated subscribers	1. The mobile security market is during the introduction period, clients are more willing to use free software, but the idea of "free basic service + charge for value-added service" is still facing difficulties. 2. The lack of market advertising leads to low recognition of brand by customers.

<표 2-6>（계속）

	Competitive Advantages	Competitive Disadvantages
360	1. A large scale of PC security software users, high recognition of the brand, positive effects on the mobile security products 2. The acquisition of Msafe is helpful to separately position the brand of 360 mobile safe and the brand of 360 Msafe according to the different future needs of customers 3. Pay attention to the interface design, and care about the feedbacks of customers 4. Strong media advertising	1. A new enters to the phone security industry, limited experience for this industry, low R&D, less patent technology. 2. “Free” business mode cannot guarantee the consistent development, stability and the investment of technology R&D of the company.
KingSoft	1. No pressure for relying on the return of phone security products and no liquidity pressure, more attentions to the feedbacks of products and public praise. 2. The apparent brand effects 3. Have the accumulative experience of anti-virus technology on PC	1. Functioning only as AV software, which is not meeting user demands 2. Not promoted as formal products 3. Lack of experience for developing mobile phone software
Kaspersky	1. Greater investment on R&D and good effects on anti-virus 2. Greater number of PC users with possible bundling in sales 3. Stronger internet channels 4. Internationalized brand with higher popularity 5. Stronger financial ability	1. Lack of understanding of the using habit of users; product experience needs to be improved 2. Not enough details of firewall and real-time monitoring 3. The standard product pack cannot meet the customers’ diversification and individuation, increase the level of requirements for new users 4. Lack of WAP channels 5. Mobile security is not the core business for development

<표 2-6>（계속）

	Competitive Advantages	Competitive Disadvantages
Rising	1. Obvious brand effect 2. Greater number of PC users, with possible bundling in sales 3. Rich entity and internet channels	9. Slower product development and inadequate attention
Jiangmin	1. Less occupied memory	1. Functioning only as AV software, which is not meeting user demands 2. Offline update only, no functions such as real-time monitoring and firewall 3. Lack of investment
F-Secure	1. Stable cooperation with Nokia	1. Weaker local channels：No portal for the download of mobile version on the Chinese main website, and no Chinese WAP web page for the customers' connection 2. Functions are not comprehensive, poor user experience
Symantec	1. Has rich experience for enterprise-level of security product technology accumulation and experience of cooperation	1. Slow localization, the mobile security research center has been moved to India from China
McAfee	1. Earlier entry to China market; internationalized brand popularity 2. Sable cooperation in PC AV with China Telecom will bring positive effect in mobile security cooperation	1. Slower product development and inadequate attention 2. Lack of investment
	3. Stronger internet channels 4. Internationalized brand with higher popularity 5. Stronger financial ability	cannot meet the customers' diversification and individuation, increase the level of requirements for new users 4. Lack of WAP channels 5. Mobile security is not the core business for development

3. 중국 모바일 보안시장 환경 분석

(1) 정부로부터의 정책지원

현재까지 중국 정부는 모바일 보안을 대상으로 한 어떠한 연관법규나 규제도 공식화하지 않았다. 그러나 중국 내 모바일 휴대전화산업의 급속한 성장에 따라 모바일 보안문제는 점점 크게 부각되고 있다. 모바일 플랫폼의 개방화가 이어지고 각종 3G 기반 편의 서비스는 증가하는 반면 휴대용 통신기기의 부족한 보안기능, 그리고 모바일 보안에 대한 일반 소비자의 저조한 인식은 향후 모바일 휴대전화로 인한 대형 보안사고를 유발할 여지를 만들어주고 있다. 이외에도 스팸 메시지나 광고전화, 무단 금융결제 소프트웨어 등은 현재도 소비자들의 불만과 혼란을 야기하고 있어 중국 정부의 관심사안 중 하나가 되고 있다.

2010년 6월 25일 열린 2010년 중국 모바일 보안업계 포럼에 참석한 중국 산업기술부 대변인은 이미 해당 부처가 일련의 정책 및 규제를 도입하고 기술연구 및 시장환경에 대한 점검을 시작했으며 모바일 정보 관리방침과 인터넷 정보서비스 관리방침을 수립했음을 밝힌 바 있다. 이러한 일련의 조치는 향후 모바일 보안 관리에 대한 정책 가이드라인을 제공할 것이다. 또한 산업기술부 당국은 모바일 보안문제를 해결하고 관리감독 기능을 강화하기 위해 향후 산업사슬 참여자들과의 공조아래 보다 합리적이고 효과적인 정책을 도입함과 동시에 중국 모바일 산업의 내실 있는 성장을 위해 적절한 기준을 제시할 것이라 밝혔다.

산업기술부는 또한 모바일 보안 산업사슬 참여자들에게 다음과 같은 사항을 주문했다. 첫째, 각 참여자는 시장의 수요에 맞추어 철저한 조사 및 표준 연구를 수행하여 산업 전반의 성장패턴에 필요한 기본 요구사항 및 소비자층의 요구사항을 파악하고 반드시 독자적 혁신을 추구해야 한다. 기술표준에 대한 연구를 보다 적극적으로 수행하여 실제 제품에 가급적 신속히 반영되도록 하고 소비자들의 수요에 대응할 수 있도록 해야 한다.

둘째, 혁신적인 핵심기술을 개발하고 현행 표준 시스템을 지속적으로 개선해야 한다. 모바일 증권거래 시스템의 설계에 특별히 관심을 기울여 필요한 부분에 확실한 우선순위를 부여하고 일원화된 설계 기획이 이루어지도록 하며, 모바일 증권거래에 사용되는 원천기술에 대한 연구개발 역량을 강화해야 한다. 또한 모바일 증권거래 시스템을 위한 과학적이고 합리적인 표준안을 개발하며 해당 서비스의 기능을 보완할 수 있는 강력한 기술표준을 제시해야 한다.

셋째, 산업사슬 내 각 부문간 공조를 강화하며 각자의 역량을 융합시키도록 해야 한다. 모바일 보안은 통신사업자, 단말기 제조사, 모바일 증권거래 소프트웨어 개발사, 사용자 및 기타 다양한 참여자가 모두 관여된 문제임을 인식하고 각 참여자가 자원을 공유하며 상호 협력, 상보적 관계를 구축하여 중국 모바일 휴대전화산업의 건전한 성장을 추구한다.

상기와 같이 중국 당국도 모바일 보안문제에 대해 높은 관심을 보이고 있다. 모바일 보안업체 역시 관련규제 및 표준안 수립에 적극적으로 참여하고 소비자들의 요구사항을 보다 활발히 파악해 수용하며, 지속적으로 기술수준 향상에 노력함과 동시에 산업사슬 참여자간의 공조체계를 강화해 중국 모바일 휴대전화산업의 견실한 발전과 진흥에 참여할 필요가 있다.

(2) 스마트폰의 급속한 보급

스마트폰은 음성통화, 멀티미디어, PC를 한데 융합하는 이른바 제3의 네트워크 통합의 방향으로 나아가며 향후 5년간 더욱 더 대중화될 것이다. 스마트폰은 무선 인터넷을 이용한 업무 및 오락기능으로 대변되는 강력한 활용도를 제공하므로 일반 사용자들에 대한 확실한 파급효과를 지니고 있다. 스마트폰의 가격 또한 점차 하향되고 있어 진입장벽이 낮아지고 있다. 스마트폰의 사용자층과 판매량이 빠르게 늘어가고 있다는 것은 물론 유익한 일이다. 게다가 안드로이드와 같은 스마트폰용 OS 플랫폼의 개방화에 힘입은 다양한 애플리케이션의

등장은 앱 개발자들이 사용자들의 여러 가지 요구사항에 맞춤형으로 대응 가능한 다채로운 유형의 앱을 개발하도록 이끄는 동력으로 작용할 것이며, 스마트폰을 이미 사용하고 있는 소비자들에게도 지속적인 구매동인으로 어필할 것이다.

써드-파티 SW에 대한 안드로이드 플랫폼의 개방성과 무료 서비스 덕택에 향후 스마트폰 개발에 대한 업계의 전망은 일반적으로 매우 낙관적이다. 주요 단말기 제조사들도 안드로이드 스마트폰의 출시를 이어가고 있으며, 일례로 LG전자 역시 2010년 상반기 안드로이드 기반의 LU2300, SU950/KU9500 및 옵티머스 등의 스마트폰을 차례로 선보였다. 이러한 보급형 스마트폰의 출시는 안드로이드 OS가 고급형 스마트폰 시장뿐 아니라 중저가 제품 시장까지도 확산되는 추세를 잘 보여준다. 보급형 스마트폰에도 구글이 제공하는 각종 서비스와 앱 다운로드를 위한 안드로이드 마켓 등 안드로이드 OS의 기본기능은 모두 제공되므로, 이러한 중저가 스마트폰이 계속 출시되면 음성통화와 문자메시지 전송기능만을 가진 저가형 휴대전화 시장은 더욱 약화될 수밖에 없다. 모바일 휴대전화 사용자들은 더욱 더 모바일 IM 소프트웨어를 사용해 소통하고자 할 것이고, SNS나 모바일 검색을 활용하며 GIS 쿼리를 이용한 위치정보를 활용하려 할 것이다. 따라서 안드로이드 플랫폼은 향후 스마트폰의 대중화를 전면에서 이끌 강력한 동력이다. 안드로이드 플랫폼을 탑재한 스마트폰은 중저가 시장을 노리며, 해당 시장은 그간 노키아 S40이 사실상 독점한 상태였으나 이제는 심비안 플랫폼 전체가 안드로이드의 강력한 도전 앞에 직면해있다. 게다가 노키아는 고가 모델과 중저가 모델 제품군 모두의 영역에서 입지가 흔들리고 있다. 다수의 관계자들은 안드로이드의 급속한 확산과 발전이 향후 수년간 이어지며 심비안의 시장점유율을 상당부분 잠식할 것으로 전망하고 있다.

<표 2-7>에는 각 스마트폰 OS의 장단점이 요약되어있다. <표 2-7>의 장단점 비교를 근거로 프로스트&설리번은 향후 전개될 스마트폰 OS 경쟁추이와 각 모바일 보안업체들의 대응전략을 <표 2-8>과 같이 전망하고 있다.

<표 2-7> The Advantages and Dsiadvantages of Smartphone OS'

Operating System	Advantages	Disadvantages
Android	1. The complete openness of platform and encourage developers to develop all kinds of applications and free of charge, low cost for the developer 2. Emphasis on the feedbacks and experience of users 3. High degree of binding between Android operating system and the mobile internet 4. More and more handset vendors (Motorola, HTC, Samsung, etc) introduced smartphones using Android system. Moreover, e-books, tablets PC and other products starts to use Android system as well. 5. The price of Google's android phone is dropping very fast, and other manufacturers have introduced low-end smartphone with Android platform as well, it is suitable for those young but price sensitive user focusing on experience of mobile operation.	Each handset vendor of Android platform wants to advance their product competitive advantages by using Android as their own API. They can change some of the underlying structure to develop some unique features, and accordingly require the security companies to follow these changes to customize the final products, which is hard for R&D and business cooperation.
iPhone	1. Because the most priority is the users' experience, products is pursuit by the global users, simple operation 2. The global sales of iPhone and iPad is increasing dramatically 3. App Store has various application for users to download 4. iPhone OS maybe open to some extent (the current degree of openness is as yet known), which is helpful to enhance its market share	iPhone in China is expensive which limits the number of users growth and China Unicom has in-apparent effects of promotion of iPhone

<표 2-7>（계속）

Operating System	Advantages	Disadvantages
Symbian	1. At present, the market share of Symbian platform is still the highest and has the largest number of Nokia smartphone users. 2. To strengthen the development and look for the developer globally for the purpose of maintaining the market share operating system and the mobile internet	1. The downward trend of market share is clearly declining 2. The bad feedbacks from Symbian users: dull UI and boring operation
Windows Mobile	1. The help from technology, brand influence, financial support and other powerful advantages of Microsoft 2. Windows Mobile 7.0 comes into market, which is likely to enhance the share in smartphone operating system market for WM	1. The market share of Windows Mobile has been low all along 2. Too emphasis on the technological and professional operation, neglect the experience of users and gradually being marginalization 3. Because of the licensing fee, mobile producers and developers is easily leaning to the system with free of charge due to the consideration of cost 4. Under the current circumstances that competitors are seizing the market share of smartphone, WM lags behind to its rivals due to the delayed release of WM7.0

<표 2-7>（계속）

Operating System	Advantages	Disadvantages
MeeGo	1. Nokia has the largest number of smartphone users and strong brand influence, which is helpful to explore the market for MeeGo and gain more user experience 2. Jointly build by Nokia and Inter, powerful alliance and strong technology. Inter also frequently shows MeeGo system 3. MeeGo as a more open Linux system, gained more support from IT enterprises, the design is aiming at a variety of hardware platforms of computing facility, including laptops, netbooks, tablet PCs, multimedia phones, network TVs and in care infotainment systems	1. MeeGo is still a complete new system, the stability of the new system and the feedbacks from customers are still unpredictable 2. Nokia is facing tough challenges in high, medium and low-end smartphone market segments.
Blackberry	The mobile phones of Blackberry are welcomed by European and American users, because of its outstanding business features	1. Blackberry has not officially entered China due to the lack of user foundation 2. The operating system is prohibited to be cracked, which is still a huge obstacle for application development 3. Due to the issue of network security, Blackberry is resisted by many countries and regions

<표 2-8> Future Competitiveness of Smartphone OS' and Responding Strategies of Major Mobile Security Vendors

Operating System	Future Competitiveness	The demand for the mobile security products	The responding strategy of each mobile security vendors
Symbian	The largest market share can be maintaining for a long time, especially the advantages of market share in low-end market	In the period of large market share, the demand for the mobile security product is still considerable	To maintain the current R&D and maintenance, but can no longer only focus on Symbian
Android	The openness brings sharp increase of market share, the future outlook is well predicted by the insiders	1. Open platform leads to more attacks from hackers, so the pace of Android facing larg-scale of threats is faster 2. Each handset vendors developed personalized features on the baisis of openness, the requirements for security is getting more diversified	The platform of Android Is the priority target for mobile security vendors. Vendors should also increase the level of R&D for Android platform products and concern about the development and feedbacks of smartphone with Android platform, then enhance the strength of promotion for competing the new smartphone users

<표 2-8>（계속）

Operating System	Future Competitiveness	The demand for the mobile security products	The responding strategy of each mobile security vendors
iPhone	Continue to maintainthe rapid growth, but the high sale price restricts the development in China	1. Users frequently download and use various applications, so they are deserved more for mobile security 2. The increasing sales will definitely attract attentions to those benefit-driven hackers	On one side, China market for iPhone maintains a high concerns, and preparation can be expected if the R&D allows to do so; on another side, for those mobile security vendors with international views, the security product for iPhone is the most important aspects for R&D, especially for European and American markets, otherwise, they tend to lag behind the local mobile security vendors.
Windows Mobile	The effects after Windows Mobile 7.0 is listing in the market can determine whether the decision of WM for the competition of operating system is successful or not	If the market response is good, then the market share of WM can be improve, there is certain demand for mobile security	Keep attention to WM 7.0, for those developers less cost sensitive and under the allowance of R&D, they should develop security product for WM 7.0, but do not require put into large efforts to R&D recently
MeeGo	Powerful alliance of new generation of smartphone, on the basis of strong support, gradually replace Symbian, more opportunities than challenges	After the list of smartphone with MeeGo platform, there is a large possibility that MeeGo can have a large number of users , therefore, the demand for mobile security products can be large	Concern on the meaningful steps of the replacement of Symbian by MeeGo, grasp the key time point for the investment of R&D efforts
Blackberry	Currently do not see any development opportunities in China	The closed system establishes a natural barrier, causes low demand for mobile security	Remain the wait-and-see attitude for Blackberry

(3) 데이터 서비스 및 모바일 네트워크의 발전

2009년부터 현재까지 통신사업자들의 음성통화 서비스 수익 및 총 수익은 꾸준히 감소하고 있는 반면 데이터 서비스의 비중은 계속 상승 중이며, 이러한 비율의 변화는 앞으로도 이어질 것으로 보인다. 앞으로 수년간 데이터 서비스의 유형은 더욱 다양해질 것이며 사용자수도 급속히 증가할 것이다. 3G 통신망의 본격화 이후 통신사업자들은 모바일 인터넷의 대중화에 더욱 앞장서고 있는데, 모바일 인터넷의 발전에는 반드시 양질의 애플리케이션이 필요하다.

현 시점에서는 온라인 게임과 모바일 SNS, 모바일 결제 등이 효과적인 구심점이다. 개인 사용자가 단독으로 이용할 수밖에 없는 오프라인 게임과 달리 모바일 휴대전화를 이용한 온라인 게임은 소셜 커뮤니케이션이라는 보다 고차원적인 만족감을 제공한다. 낮아진 진입장벽을 토대로 모바일 온라인 게임의 수용성은 점진적으로 향상될 것이다. 모바일 게임의 인기가 높아질수록 모바일 게임 사용자들로부터의 민감한 개인정보 및 결제수단에 대한 보안 수요도 폭증할 것이다.

모바일 SNS 역시 새로운 형태의 네트워크 개발을 주도할 강력한 흐름이다. 현재 Tencent는 기존의 SNS 커뮤니티를 모바일 인터넷으로 이전하고 있으며 사용자 인터페이스 역시 모바일 인터넷에 맞게 개선하고 있어 Tencent에 대한 사용자들의 유대감을 강화시키고 있다. 또한 SNS 역시 계정 정보나 암호, 각종 개인정보와 연락처 정보 등 매우 민감한 프라이버시 영역에 속한다는 점을 상기해야 한다. 따라서 모바일 SNS의 발달에 발맞추어 개인정보 보안 수요에 신속히 대응해야 한다. 모바일 전자상거래나 모바일 결제 역시 사용자들의 금융자산과 직결된 문제이므로 계좌정보나 비밀번호를 보호할 강력한 수단 마련이 필요하다. 다시 말해 데이터 서비스 및 모바일 인터넷의 발달은 곧 다양한 애플리케이션에 걸친 사용자 정보 보안에 대한 수요 증대로 이어질 것이다.

(4) 3G 통신망의 구축 및 확대

3대 주요 3G 통신사업자들의 인프라 투자와 마케팅은 점점 더 강화되고 있다. 와이파이나 3G 통신망을 이용한 모바일 휴대전화 사용자들의 모바일 인터넷 사용량 증가는 모바일 보안을 중대한 화두의 하나로 격상시켰다. 3G 통신망 구축에 대해 중국 산업기술부는 2010년 3월 다른 7개 부처와 공동으로 '제 3세대 모바일 통신망 구축 및 진흥에 대한 의견'을 발표한 바 있다. 해당 문서에는 중국 내 모든 주요도시와 마을, 고속도로 및 관광지에서 3G 네트워크를 사용할 수 있게 될 것이라 언급한 바 있으며, 현재까지 총 30만개의 3G 기지국이 세워져 수 자체로만 보면 거의 최종 단계에 와있다고 할 수 있다. 인프라 자체에 대한 투자는 이제 활발히 진행중인 네트워크 최적화 및 성능 개선작업, 네트워크 및 정보 보안 향상 등으로 방향을 옮겼다. 정부 당국은 통신사업자들의 경쟁력이 시장에 의해 갖추어져야 한다고 보고 이를 독려하고 있으며, 산업사슬 전반에 걸친 공조체제를 마련하고 3G 통신망 및 모바일 인터넷을 위한 혁신적인 서비스를 개발함과 함께 다양한 애플리케이션을 선보여 자연스럽게 통신망 업그레이드를 견인하도록 할 것을 주문하고 있다.

(5) 모바일 휴대전화 바이러스 대란

2009년에는 약 1천 종의 모바일 휴대전화 바이러스가 확인된 바 있다. 특별히 대규모 혼란을 야기하거나 사회경제적 피해를 유발한 모바일 바이러스는 없었으나, 2010년 상반기에 들어서자 모바일 바이러스의 종류는 2~3배 폭증했다. 'Mobile Phone Skull'이나 'Straight Flush Thieves' 등이 좋은 예다. 특히 전자의 경우 수십만 대의 스마트폰을 감염시켜 약 2천만위안에 달하는 막대한 금융 손실을 야기했다. 이렇듯 모바일 바이러스는 2010년 빠른 속도로 확산되며 사회경제적 문제로 인식되기 시작했다. 2010년 한 해 발견된 바이러스 및 악성 소프트웨어만 2천 2백여가지에 달해 그 유형도 빠르게 다양해졌다. 향후에는 더욱 심각한 모바일 바이러스 대재앙이 닥칠

가능성도 상존해있다.

스마트폰의 대중화와 OS의 개방에 따라 바이러스 대응 및 전파환경 연구를 위한 투자가 절실하다. PC와 비교해 모바일 휴대전화는 요금 지불과 직결되어있으므로 개인정보와 프라이버시를 담고 있기에 모바일 바이러스를 통해 이윤을 무단 취득하려는 행동을 유발할 수 있다. 모바일 바이러스에 대한 관심 역시 연쇄적으로 커지고 있어 대규모 사건사고로 이어질 가능성은 점점 커지고 있다. 이른바 봇넷에 대한 모바일 바이러스 논의를 바이러스 개발, 유통, 과금 채널에 이르기까지 이른바 '검은 산업사슬'이 여러 산업영역에 걸쳐 존재하고 있다.

또한 그간 여러 유형의 모바일 인터넷 앱이 매우 빠른 속도로 개발된 까닭에 모바일 데이터의 저장이나 전송, 모바일 결제용 계정 비밀번호, 이용요금 등 모바일 바이러스가 침투할 수 있는 영역도 그만큼 다변화됐다.

스마트폰 OS인 심비안과 안드로이드의 개방성도 꾸준히 높아져왔기 때문에 해커들이 바이러스를 개발하고 OS의 핵심영역에 바이러스를 이식할 수 있는 위험성도 함께 상승했다. 따라서 앞으로는 OS 자체의 보안을 확보하는 것도 매우 중요한 도전과제가 될 것이다.

(6) MID 제품 및 IoT의 발전

기술이 발전하면서 모바일 인터넷용 보조제품은 스마트폰을 넘어 통신 기능을 갖춘 다양한 종류의 모바일 인터넷 기기(Mobile Internet Device: MID)로 확산될 것이다. 2010년 4월 중국에 아이패드가 출시된 이후 2010년 6월 말 판매량은 이미 3백만대를 넘어섰고, 2010년 말에는 약 1천만대를 돌파한 것으로 예상되고 있다.

아이패드는 인터넷 서핑의 편의성, 앱과 콘텐츠의 다양성 등으로 사용자들에게 크게 어필했고, 아수스와 에이서 역시 당해 4분기에 타블렛 PC를 선보였다. 한편 MID 제품의 선두주자로 꼽히는 타블렛 PC 역시 다양한 모바일 인터넷 앱을 설치해 사용한다는 점에서 동일한

보안 문제를 안고 있다. 향후 MID 사용자들이 대폭 증가할 경우 역시 모바일 보안제품에 대한 수요도 함께 늘어날 것으로 전망된다. 따라서 모바일 보안업체들은 MID용 제품 개발에 관심을 갖고 보안 위험 동향을 주시하며 적시에 사용자들에게 보안 서비스를 제공할 수 있도록 준비해둘 필요가 있다.

2010년 말, 중국 산업기술부는 TD-SCDMA와 사물 인터넷(IoT: Internet of Things)의 융합이 중국 내 업계 전반과 정보통신 인프라의 통합을 촉진할 것이고, IoT 분야의 빠른 전개가 TD 분야에 커다란 기회를 제공할 것이라는 전망을 내놓았다. 현재 3대 주요 통신사업자들은 IoT에 대한 전략개발을 시작하는 단계에 있다. M2M은 이미 여러 산업분야에 걸친 개발 청사진을 대략적으로 수립했으며, 앞으로 IoT 개발이 계속해서 진행됨에 따라 보다 많은 OS 및 산업기기용 통신기능이 일반 소비자들의 일상과 더욱 가까워질 것으로 전망된다. 모바일 휴대전화가 IoT 차원에서도 매우 중요한 의미를 갖는 제품임을 감안하면 모바일 보안에 대해서도 분명히 강력한 기준이 만들어져야 하며, 계속해서 새로운 영역을 위한 모바일 보안제품 수요가 발생할 것이다.

(7) 모바일 휴대전화용 금융 서비스의 급속한 발전

중국 공상은행(ICBC)은 2008년 말부터 모바일 WAP 뱅킹 서비스를 개시함으로써 본격적인 손 안의 모바일 금융서비스 시대가 열렸음을 알렸다. ICBC의 모바일 폰뱅킹 (WAP) 서비스를 사용하면 휴대전화의 WAP 브라우저를 이용해 각종 금융서비스 요청 및 송금 서비스, 모바일 휴대전화간 전송, 각종 지출내역 관리, 펀드 및 기타 금융자산 관리 등을 수행할 수 있어 일상 속에서의 금융서비스에 대한 편의를 도모하고 간편한 휴대기기를 이용해 재테크 관리 요구에 대응할 수 있다. 2008년 말 ICBC의 모바일 뱅킹 서비스 이용자는 3백만명에 그쳤으나, 2009년에는 그 수가 2천만명으로 늘었다. 또한 2010년 말에는 약 6천만명을 넘어선 것으로 예상된다. 모바일 뱅킹의 빠른 확산 역

시 금융서비스에 대한 보안 문제를 반드시 수반할 수밖에 없다.

Taobao 역시 2008년 스마트폰 서비스를 출시했으나, 네트워크 측면에서 준비가 미진했던 탓에 처음에는 무선 네트워킹 순위에서 크게 뒤처졌다. 2010년 해당 서비스(m.taobao.com)의 트래픽은 일일 약 3천만건이었고, 이 가운데 금융거래는 1천만건이었다. Taobao 모바일 휴대전화 순위도 함께 상승했다.

4. 중국 모바일 보안시장 동향 및 기회 분석

(1) 제품 동향

① 백신, 개인정보 보호, 데이터 보호가 보안제품의 3대 주요기능으로 자리잡을 것

2010년 한 해 동안 모바일 휴대전화 대상 바이러스와 악성 소프트웨어의 수는 기하급수적으로 증가했고, 향후 1~2년 내 모바일 바이러스 대란이 벌어질 수도 있을 것으로 우려된다. 사용자들의 데이터 서비스 사용시간 및 그에 대한 의존성이 증가하면서 악의를 가진 해커들의 관심을 끌기에 충분해진 것이다. 개방형 OS 환경도 바이러스나 악성 소프트웨어가 개발될 수 있는 많은 여지를 제공하고 있다. 게다가 개방된 무선 인터넷 통신망 및 고속 3G 네트워크 역시 모바일용 애플리케이션 환경의 보안을 위협하고 있다. 따라서 모바일 휴대전화의 백신 기능은 여전히 모바일 보안제품 개발에 있어 빼놓을 수 없는 주요 고려요소다. 모바일 휴대전화 제조사들은 계속해서 백신 DB를 업데이트하고 보안기능을 강화할 필요가 있으며, 향후에는 클라우드형 백신이 모바일 백신기술의 주요 화두로 자리잡을 가능성도 감안해야 한다.

동시에 스팸 메시지나 광고 및 사기성 SMS, 보이스 피싱 등도 여전히 심각한 수준이며 사용자들의 수용성 역시 점차 떨어지고 있다. 따라서 이러한 요인들로부터 사용자를 좀더 안전하게 보호하고 일상생활에서 안심하고 모바일 휴대전화를 사용할 수 있도록 할 제품이 필요하다. 모바일 휴대전화의 프로세서 성능은 계속해서 강화되고 있

어 향후 더욱 중요하고 민감한 개인정보를 취급하는 허브 역할을 수행하게 될 가능성이 크다. 따라서 모바일 보안제품의 데이터 보호기능도 그에 발맞추어 더욱 강화되어야 할 것이고, 종국에는 모바일 휴대전화로 수행하는 모든 프로세스에 데이터 보호가 적용되도록 해야 한다. 또한 휴대전화를 분실했을 때 개인정보를 보호할 수 있는 통합형 서비스도 필요하다. 향후에는 모바일 휴대전화 자체의 보안뿐 아니라 기기의 사용과정 및 분실 상황에서까지도 데이터를 보호함으로써 사용자들이 안심할 수 있는 서비스를 제공해야 할 것이다. 그러한 관점에서 보면 데이터 보호기술 부문의 성장 잠재력은 매우 크다.

② 모바일 보안제품 동향은 사용자들의 잠재적 요구사항과 애플리케이션 통합이 주도할 것

현재는 모바일 보안제품이 백신, 개인정보 보호, 데이터 보호 영역에 머물러있지만, 앞으로는 제공 기능의 종류와 기술적 수준에 있어 더 많은 발전이 필요하다. 우선 사용자들의 모바일 휴대전화 사용 시나리오와 심리에 대한 심도 있는 연구를 통해 핵심 요구사항 및 주요 사용자 그룹의 특성을 분명히 파악하고, 이후 사용자들의 요구에 맞게 기술 R&D에 대한 투자를 늘려야 한다. 또한 애플리케이션 통합이라는 대전제 아래 향후 더욱 다양한 앱들이 개발단계부터 좀더 섬세한 부분까지 보완하여 사용자 경험과 편의성을 향상시킬 필요가 있다. 이러한 노력들은 특히 모바일 휴대전화 시스템의 관리 및 최적화와 개인 계정정보 시스템, 그리고 각기 다른 모바일 애플리케이션을 위한 보안 서비스 등에 많은 긍정적인 영향을 줄 수 있을 것이다.

(2) 채널 동향

① 다운로드 경로로는 여전히 인터넷과 WAP가 강세

현 시점에서 SW 다운로드에는 인터넷과 WAP 웹사이트가 가장 널리 사용되는 채널이며 모바일용 SW에도 상황은 동일하다. 향후 1~2년에 걸쳐 검색, 다운로드, 결제 및 각종 사용환경과 서비스 편의성이

높아지면 모바일 보안 SW 다운로드 채널 역시 해당 채널들에 머무를 전망이다. 스마트폰 판매량이 계속 늘어나는 상황을 감안하면 보안제품 제조사들은 인터넷 및 WAP 웹사이트와의 협력 아래 마케팅 활동을 펼쳐나가야 할 것이다.

② 단말기 사전 설치형 및 통신사별 맞춤형 보안 솔루션도 증가세에 있어

모바일 보안사고의 증가에 따라 모바일 보안수요도 계속해서 늘어나고 있다. 단말기 제조사와 통신사들은 모바일 보안의 중요성과 심각성을 인식하고 주요 모바일 보안업체들과의 협력관계를 강화하고 있으며, 이 과정에서 모바일 보안용 SW를 휴대전화에 사전 설치하는 방식을 취하고 있다. 또한 모바일 보안 산업사슬 내에서 단말기 제조사와 통신사가 차지하는 역할 비중도 갈수록 커질 전망이다.

모바일 보안업체가 신형 휴대전화에 보안용 제품을 사전 설치하거나, 신제품 출시에 맞추어 다른 참여자와 합작해 판촉활동을 펼친다면 제품 활성화 비율을 더욱 끌어올릴 수 있을 것이다. 또한 동일한 유형의 휴대전화를 구매하는 소비자들은 유사한 소비 패턴을 보이므로, 동종 휴대전화 구매자에 대한 마케팅 활동을 보다 공격적이고 지속적으로 펼친다면 만족스러운 투자대비 효과를 얻을 수 있을 것으로 전망된다.

통신사들 역시 모바일 보안제품의 지속적인 개발에 관심을 가져야만 한다. 모바일 보안업체와 이동통신 사업자간에는 다양한 형태의 협력체제가 가능하다. 첫째, 보안제품이 사전 설치된 맞춤형 휴대전화를 통해 부가가치를 끌어올리는 모델이 가능하다. 둘째, 휴대전화 제조사가 통신사에 일정 수준의 서비스를 제공함으로써 특정 기능에 대한 보안제품 개발을 지원하는 것도 가능하다. 주요 통신사들은 마케팅 활동 전반을 관장하고 있으며 방대한 사용자층과 성숙단계에 있는 채널을 보유하고 있으므로 홍보 효과도 극대화할 수 있을 것이다. 셋째, 모바일 보안 서비스를 사용자들에 대한 하나의 부가가치 서비스

로 취급하여 패키지 또는 번들 상품에 편입시키는 모델도 가능하다. 통신사들은 SMS나 MMS 전송, WAP 푸시, 포털 사이트 등 영업 및 판촉을 위한 다양한 자원을 보유하고 있으므로 이를 활용할 수 있다. 또 모바일 보안업체가 펼치는 마케팅보다는 통신사가 직접 수행하는 마케팅이 훨씬 큰 파급효과를 지닐 수 있다. 넷째, 모바일 보안업체들이 통신사 자체의 네트워크에 대한 보안 서비스를 제공하는 방식도 생각해볼 수 있다.

③ CP, SP 및 기타 업계 사용자간 혁신적 공조 기대해야

모바일 애플리케이션 산업사슬 내 모든 참여자들이 모바일 보안에 촉각을 곤두세우고 있는 상황임을 감안하면 향후 모바일 보안업체를 중심으로 한 새로운 공조체제가 수립될 가능성이 크고, 그에 따라 모바일 보안제품의 홍보를 위한 신규 채널이 형성될 수 있다. 은행을 예로 들면, 모든 은행들이 모바일 폰뱅킹 및 전자지갑 서비스를 출시하고 있는 상황에서 계좌, 비밀번호 및 결제 프로세스에 대한 모바일 뱅킹 보안수요가 폭증할 것으로 충분히 예상할 수 있다. 따라서 휴대전화 제조사는 모바일 폰뱅킹 서비스 이용자를 위한 각종 보안결제용 보호 플러그-인 서비스를, 모바일 보안업체는 SP, 웹사이트 및 네트워크 장비업체를 위한 다양한 플러그-인 서비스를 제안할 수 있을 것이다.

현재는 모바일 보안업체와 업계 사용자간 협력이 여전히 초기단계에 머물러있으나, 업계 사용자들의 인식이 더욱 높아지면 해당 시장이 본격적으로 개발단계에 접어들 것이다. 향후 3년 이내에는 새로운 협력 모델을 강구해야 할 필요성이 대두될 것이다.

(3) 경쟁 추이

① 모바일 보안시장 향후 경쟁 동향 전망: 참여자간 경쟁은 더욱 치열해질 것이며, 사용자의 다양한 요구에 대응할 수 있는 최상의 서비스를 제공하는 업체만이 살아남을 수 있을 것이다. 또한 선도

업체가 전체 시장의 50% 이상을 점유할 가능성이 크다.

2010년 한 해 동안 모바일 바이러스와 악성 소프트웨어는 큰 폭으로 증가했으며, 1~2년 내 모바일 바이러스 대란의 가능성까지 점쳐지고 있는 상황이다. 따라서 모바일 보안업체들은 치열한 경쟁을 준비하고 있으며, 시장점유율을 선점하기 위한 각축은 이미 시작된 지 오래다. 더구나 중국의 모바일 보안시장의 빠른 발전속도를 감안하면 향후에도 더 많은 업체들이 경쟁에 참여할 것으로 예상해야 한다. 국내외 선도적 모바일 보안업체와 기존 PC 보안업체들은 각기 저마다 다른 전략으로 중국 모바일 보안시장에 진출하려 할 것이다. 이처럼 경쟁이 치열해질 경우 유일한 생존전략은 결국 어느 업체가 사용자들의 요구에 가장 성공적으로 대응하느냐가 될 것이다.

모바일 보안제품 시장은 현재 도입기 후반에 접어들었다. 전체 사용자수는 아직 적은 수준이나, 주요업체들은 이미 상당수의 사용자를 확보하고 있는 상황에서 모바일 보안업체간 경쟁은 더욱 복잡한 양상을 띨 전망이다. 모바일 보안업체들은 현재 서로 상이한 전략을 통해 사용자들에게 어필하고 있는데, 어떠한 방식으로건 스마트폰의 판매량 증가를 활용해야 할 것으로 보인다. 이미 상당수의 사용자를 확보한 주요업체들은 기존 고객층을 유지하기 위해서뿐만 아니라 신규, 기존고객의 차별 없이 보다 다양한 혜택과 할인상품을 제공해야 할 것이다. 또한 근본적으로 사용자들의 핵심 요구사항을 정확히 파악하고 전반적인 사용자 경험을 향상시킴으로써 경쟁력을 유지해야 할 것이다.

모바일 보안제품이 보호해야 할 대상은 이제 휴대전화 자체만이 아니라 휴대전화 사용 프로세스 및 분실, 도난 시나리오까지 포함된다. 따라서 보안업체들은 모바일 보안의 안전성과 편의성 강화를 위해 보다 통합적인 형태의 솔루션을 제시해야 한다. 그러려면 꾸준한 R&D 투자와 사용자층 확보, 사용자 요구사항 파악 및 사용자 경험에 대한 고민이 뒤따라야 하고 산업사슬 내 다른 참여자들과의 새로운 동반협력 모델을 구축함과 동시에 브랜드 이미지 강화 등과 같은 마

케팅 활동도 펼쳐나가야 한다. 휴대전화 시장 경쟁에서 이러한 조건을 충족시키지 못하는 모든 모바일 보안업체들은 결국 살아남지 못할 것이다. 강력한 전방위 역량을 갖추고 사용자들의 요구사항에 대응할 수 있는 업체만이 상위 입지를 고수할 수 있을 것이다. 또한 최상위를 선점하는 업체가 전체 시장의 절반 이상을 점유하게 될 것으로 전망된다.

모바일 보안업체가 시장 내 입지를 유지하려면 다음과 같은 요건을 충족시켜야 할 것이다.

1. 기본적인 모바일 백신 및 보호기능에 대한 기술을 다량 확보해야 한다. 광범위한 바이러스 DB 정보를 구축하고 업데이트를 신속히 단행하며, 클라우드 보안기술을 선도하며 다양한 유형의 스마트폰 OS에 대한 R&D와 함께 기술특허를 확보해야만 한다.

2. 다수의 사용자를 확보함으로써 새로운 바이러스 샘플 및 피드백을 입수할 수 있어야 하고, 사용자들의 핵심 요구사항을 빠르게 파악해야 한다. 또한 모바일 보안제품을 통한 안정적인 수익모델 구축을 통해 R&D 및 마케팅에 대비한 역량을 강화해야 한다. 사용자층 확보는 업계 내 다른 참여자들과의 협상을 이끌어낼 수 있는 자본이기도 하다.

3. 보안업체들은 사용자들의 실제 피드백에 더욱 귀를 기울여 요구사항을 충족시킬 수 있어야 한다. 기존의 백신 기능을 넘어 다른 보안기능까지 서비스 영역을 확대시킬 필요가 있으며, 사용자들의 피드백을 최우선적으로 반영하여 보다 상세하고 강력한 기능을 첨가해야 한다. 각기 다른 모바일 인터넷 애플리케이션의 개발은 계속해서 새로운 보안수요를 창출할 것이므로 시장의 동향을 지속적으로 예의주시하며 작은 변화도 놓치지 말고 신규수요를 발굴해낼 필요가 있다. 또한 개발역량의 유지와 강화를 위해 새로운 보안기능에 대한 R&D 투자도 게을리해서는 안될 것이다.

중국 모바일 보안시장의 빠른 성장은 앞으로 더 많은 참여자를 시

장으로 이끌 것이다. 단말기 제조사들도 직접 보안제품을 개발해 자사 모델에 적용할 가능성이 있다. 해외의 주요 PC 보안업체들 역시 모바일용 제품을 계속해서 출시할 것이며, 여타 모바일 SW 제조업체들도 시장에 언제든지 뛰어들 수 있다. 이처럼 참여자의 수가 늘어나고 유형도 다양해지면 당연히 업계 전반의 선진화와 관심도 증가에는 긍정적일 수 있으나, 모바일 보안업체들의 기본 정체성이 서로 판이하게 달라질 경우에는 부정적인 영향을 줄 수도 있을 것이다.

② PC 백신 제조사들과 비교해 모바일 보안 솔루션 전문업체의 경쟁력이 우위에 있다.

중국 내 모바일 보안업체는 크게 두 부류로 나뉜다. 하나는 모바일 보안제품만을 전문적으로 개발, 판매하는 경우이고, 다른 하나는 PC용 백신 업종에서 모바일 영역으로 넘어온 경우다.

기존 PC 백신 제조사들의 경우 PC 제품분야에서 축적한 백신 관련기술과 브랜드 파워, 자금력 및 기타 다양한 경쟁력을 지니고 있다. 그러나 모바일 애플리케이션과 모바일 사용자라는 새로운 대상에 적응하기까지는 오랜 시간이 소요된다. 모바일 보안제품 전문업체는 모바일 휴대전화 사용자들의 이용패턴을 보다 깊이 이해하고 있기 때문에 요구사항에 더욱 민첩하고 능동적으로 대처할 수 있을 것이며, 다양한 유형의 모바일 OS에 대한 제품의 일관성을 확보하는 데에도 유리할 수 있다. 또한 모바일 애플리케이션 사슬 내에 구축해둔 협력체제도 상당한 힘을 발휘할 수 있다. 따라서 모바일 보안 분야에 집중하고 수년간 해당 분야에 대한 기술적 경험을 다량 확보한 업체가 경쟁 우위를 지닐 것으로 전망된다. 시장점유율을 늘리려면 제품과 채널의 두 가지가 핵심 요소인데, 이 모두에서 모바일 보안제품에만 특화된 업체가 보다 유리할 것이다.

(4) 비즈니스 모델 동향

① 모바일 보안업체들의 장기적 전략은 '기본 서비스 = 무료, 부가가치 서비스 = 유료' 모델

현재 360과 Kingsoft, Rising 및 기타 업체들은 시장 저변확대를 위해 무료 제품을 제공하고 있다. 그러나 기업이 유지되려면 장기적으로 보다 성숙하고 안정적인 비즈니스 모델이 반드시 필요하다. 언제까지나 무료 제품만으로 지탱할 수는 없으므로 어떠한 형태로건 유료화는 필수다.

사용자들은 당연히 무료 보안제품을 선호하겠지만, 모바일 보안의 심각성이 점차 명확하게 드러나면 유료 서비스나 제품에 대한 수용성도 점진적으로 증가할 것이다. 또한 사용자들이 요구하는 것은 저마다 달라 철저한 맞춤화가 필요하므로, 단 하나의 일관된 과금정책으로는 이에 대응할 수 없다. 모바일 보안에 대한 다양한 부가가치 서비스를 제공할 경우 구매력을 갖춘 가입자들을 충분히 유치할 수 있을 것이다. 또한 유사 제품의 대량 출시로 인해 가격 및 경쟁력에 대한 부담은 점점 줄어들고 있는데, 가격의 하향은 중저가 제품을 원하는 소비자들의 진입장벽을 낮춘다는 점에서 유리하게 작용할 수도 있다. 모바일 보안제품 환경은 계속 유동적으로 변화하고 있어 사용자들은 보다 장기적인 관점에서 꾸준한 업데이트가 제공되는 제품을 기대한다. 모바일 보안제품은 한번 선택하면 계속해서 높은 신뢰도를 보이는 경향이 있으므로, 유료 서비스 모델을 유지하는 것이 크게 어렵지는 않을 것으로 전망된다.

결론적으로 향후 모바일 보안제품의 개발 동향은 기본 서비스를 무료로 제공하고 부가가치 서비스에 요금을 부과하는 형태의 비즈니스 모델이 될 가능성이 크다.

② 모바일 보안업체들이 다양한 B2B 협력모델을 추구할 것으로 전망

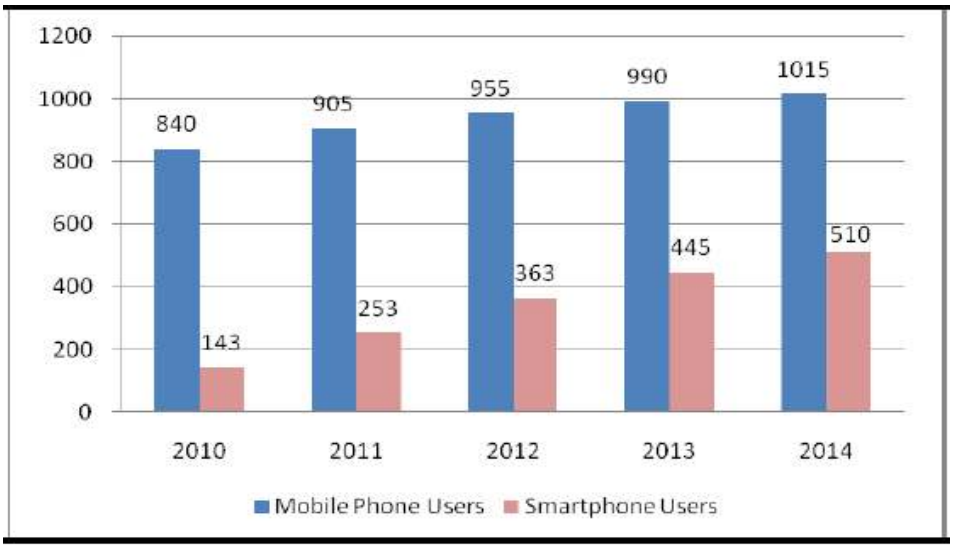
중국 내 모바일 보안업체들은 단말기 제조사, 통신사업자, 은행 및 기타 기업 고객과의 다양한 협력관계를 구축하고자 노력하고 있다. 그룹 클라이언트를 위한 제품들도 이미 출시되어있다. 3G 통신망의

활성화와 모바일 애플리케이션의 대중화가 이어지면 B2B 협력체제도 다변화, 공고화 추세로 나아갈 것이다. 모바일 보안업체들은 개별 사용자들에 대한 유료 서비스 모델을 기업 사용자층으로 확대시키기 위해 상이한 사용자 그룹에 대해 보다 통합적인 보안기능을 지원할 수 있는 방안을 모색하고 있으며, 기업 사용자들을 위한 네트워크 보안 강화기술을 계속 연구하고 있다.

5. 중국 모바일 보안시장 규모 예측

프로스트&설리번은 모바일 보안 SW 시장이 PC용 사전 설치식 보안 SW 시장과 유사한 양상을 띨 것으로 전망하고 있다. 스마트폰용 보안 SW 수요도 이에 포함된다. 따라서 스마트폰의 꾸준한 보급이 결국 모바일 보안시장의 규모와 성장속도를 결정할 것이다. 이러한 판단을 기초로 프로스트&설리번은 향후 스마트폰 사용자층의 변화에 우선 주목하고 있다. [그림 2-16]에서 보는 바와 같이 중국 내 전체 모바일 휴대전화 사용자는 계속해서 증가하고 있으나, 기존 사용자층이 누적되면서 그 증가속도는 점차 둔화되고 있다.

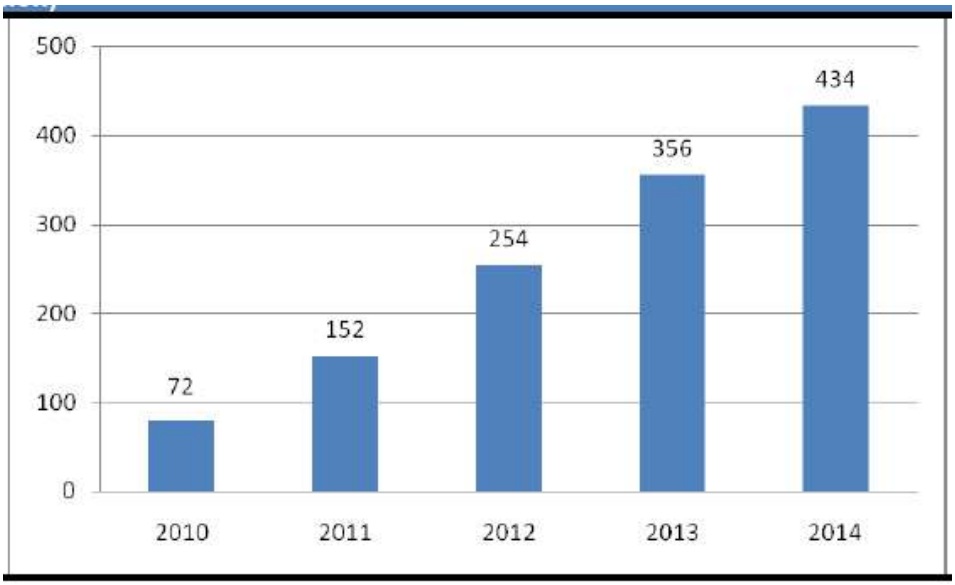
[그림 2-16] 이동전화 및 스마트폰전화 사용자수 예측(단위 백만)



전체 휴대전화 사용자 가운데 스마트폰 사용자가 차지하는 연간 비중 및 사용 비중은 약 50%에 달할 것으로 전망되며, 2014년에는 스마트폰 사용자수가 약 5억 1천만명에 달할 것으로 예상된다.

스마트폰의 대중화에 따른 모바일 보안용 SW 수요의 증가, 정부당국의 관련정책, 3G 및 모바일 인터넷의 지속적인 성장, 바이러스로 인한 크고 작은 보안사고, 사용자들의 보안에 대한 인식도 등은 저마다 모두 모바일 보안산업의 향방에 영향을 미칠 것이다. 모바일 보안산업 발전의 제반 환경에 대한 분석을 바탕으로 프로스트&설리번은 2010년 말 모바일 보안제품 활성 사용자가 7천 2백만명을 넘을 것으로 추산했으며, 시장규모는 계속해서 빠르게 확대될 것으로 전망한다. 2014년에는 중국 내 모바일 보안제품 활성 사용자 비중이 전체 사용자의 85%에 달할 것으로 예상되고 있으며, 실사용자 수는 약 4억 3천 4백만명에 이를 것으로 전망된다.

[그림 2-17] 모바일 보안제품 활성 사용자수 예측(단위 백만)



제3절 글로벌 모바일 보안시장 개황

1. 글로벌 모바일 보안 주요 이슈 개관

전세계적으로 보면 광범위하게 확산된 PC 바이러스로 인한 심각한 폐해와 달리 모바일 보안 문제는 비교적 소규모의 바이러스 유포, 악성 소프트웨어 및 스팸 메시지 등으로 국한되어있다. 그러나 스마트폰과 모바일 인터넷의 급속한 성장은 플랫폼 개방성을 증대시켰고, 그 결과 글로벌 모바일 통신업계가 보안 문제에 주목하지 않을 수 없는 단계에 도달했다. 상기 열거한 항목들과 같은 모바일 보안문제는 2010년 2월 개최된 모바일 월드 콩그레스(Mobile World Congress)에서도 의제 중 하나로 선정됨으로써 세계 각지의 통신사와 제조사들에게 모바일 보안에 대한 과제를 제시했다.

글로벌 모바일 보안 서비스 배포에 대한 지역별 전망을 살펴보면 선진국과 개도국간 각기 다른 특징을 발견할 수 있다.

■ **개발도상국 (중국, 인도네시아, 남아프리카, 중동 등)** 개도국은 높은 인구밀도와 다수의 모바일 사용자층, 그리고 저조한 PC 보급률로 말미암아 선진국에 비해 모바일 뱅킹 및 모바일 이메일 앱의 수가 더 많은 편이다. 따라서 해당 유형의 앱들로 인한 보안 문제가 더욱 빈번히 발생하고 있으나 정책 거버넌스는 상대적으로 취약하며, 그 결과 아시아, 아프리카, 남미 지역에 대한 모바일 보안 수요가 크다. 실례로 러시아에서는 모바일 바이러스가 매우 빈번하게 출몰하고 있으며, 동남아시아에서는 스팸 메시지 전송이 광범위하게 확산되어있다. 특히 심비안 OS를 지원하는 중저가형 스마트폰 사용자가 많은 동남아시아 지역에서는 모바일 보안제품의 시장 규모도 그만큼 크다.

■ **선진국 (북미, 유럽, 일본 및 한국)** 인터넷 보급률이 높은 이들 지역에서는 모바일 앱의 종류가 많지 않다. 이동통신 시장에 대한 엄격한 규제가 모바일 보안 문제의 확산을 억제하고 있는 것이다. 특히

일본과 한국의 경우 산업사슬을 통신사업자가 독점하고 있어 앱 플랫폼이 제한적이며, 따라서 바이러스나 악성코드, 스팸 등의 활동 폭이 크지 않다. 그러나 스마트 모바일의 확산 추세와 모바일 앱의 다양화, 그리고 앱 플랫폼의 개방화가 주된 흐름으로 자리잡은 상황에서 모바일 보안 역시 핵심 이슈로 부상하고 있다. 수요가 증가하면 곧 모바일 보안제품 시장 역시 성장할 가능성이 크다. 실제 한국에서는 스마트 모바일 휴대전화에 보안 소프트웨어의 사전 설치를 강제화하는 법규를 공표할 예정이다. 또한 선진국에서는 개인정보 보호에 대한 의식이 널리 확산되어 있는데, 스마트 모바일 기술이 발전할수록 개인정보 유출의 위험성도 높아지고 있으므로 선진국에서는 개인정보 보호기능을 제공하는 보안제품이 각광받게 될 것이다.

모바일 앱에 대한 기술적 장벽은 갈수록 크게 낮아지고 있으며, 앱 개발자들에 대한 아이폰과 안드로이드 시스템의 진입장벽 역시 낮기 때문에 신규 애플리케이션의 독자적 개발은 새로운 시대를 맞고 있다. OS의 일관성이 없던 과거에는 무엇보다 호환성 확보가 어려웠기에 VAS 개발이 쉽지 않았다. 반면 애플의 iOS와 구글의 안드로이드 OS는 앱 개발자들에게 호환성 고민을 덜어주고 혁신적인 아이디어를 보다 자유롭게 펼쳐낼 수 있는 여유로운 개발환경을 제공하고 있어, 결과적으로 사용자들에게는 더욱 다채롭고 편리한 모바일 소프트웨어가 공급되고 있다. 그러나 그만큼 모바일 바이러스를 개발하기도 수월해진 탓에 해커와 악성코드 유포자들도 써드-파티 앱 분야로 유입되고 있다.

유무선 인터넷의 통합과 3G 및 와이파이 통신망의 발전에 힘입어 모바일 휴대전화 환경은 더욱 광범위하고 복잡해졌으며, 그만큼 보안 위험도 역시 동반 상승했다. 클라우드 시대는 이미 목전에 도래했으며, PC 영역에서 두드러진 변화를 느끼지 못한다면 모바일 휴대전화 사용환경의 변화를 눈여겨보아야 한다. 충분한 대역폭만 확보된다면 클라우드 컴퓨팅 기술을 기반으로 모바일 휴대전화의 활용도가 크게 향상될 수 있기 때문이다. 또한 이른바 클라우드 시대를 맞아 모바일

휴대전화 보안 문제는 단말기 제조사, 통신사 및 보안 서비스 제공자들을 포함한 모바일 앱 사업자들에게 새로운 도전과제로 다가올 것이다.

2. 글로벌 모바일 보안 시장 개관

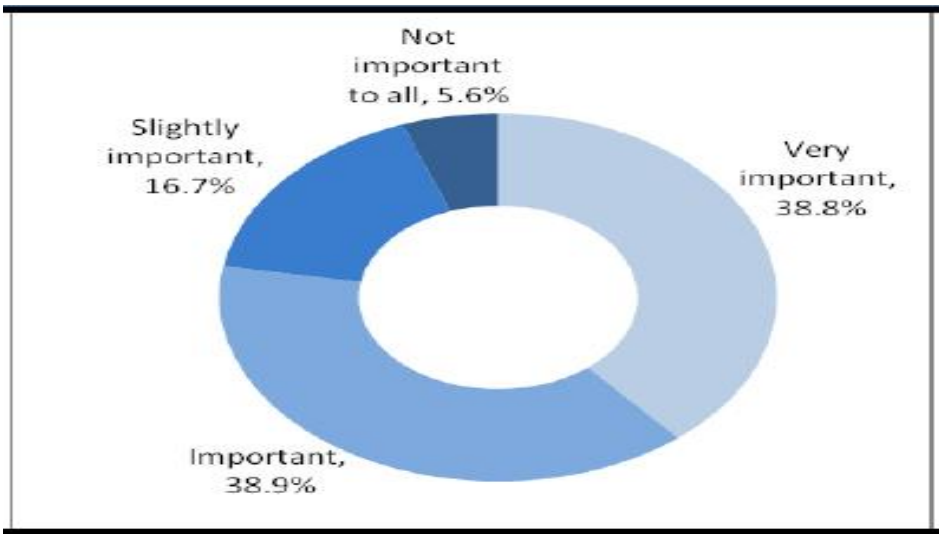
북미와 유럽 시장에서는 개인용 모바일 보안제품보다 기업용 모바일 보안 솔루션의 개발속도가 더 빠른 양상을 보인다. 기업용 모바일 보안제품은 주로 임직원들의 업무용 소프트웨어가 취급하는 데이터의 보호에 초점을 두고 있다. 직장인들이 업무용 메일 교환 등을 목적으로 사용하는 블랙베리나 아이폰 등의 휴대전화는 고용주가 제공하는 경우가 많은데, 이러한 경우 사내 영업기밀 등의 유출을 방지하고 데이터 전송의 안전성을 확보하기 위해 기업측에서 보안제품 제조사의 유료 서비스를 이용하게 되므로 자연히 모바일 바이러스가 확산될수록 기업용 모바일 백신 소프트웨어에 대한 수요도 증가할 것으로 전망되며, 모바일 보안의 주된 관심사 역시 사내 정보보호 측면에 꾸준히 맞춰질 것이다. 기업용 모바일 보안제품이 개발됨에 따라 개인용 모바일 제품의 보안에 대한 관심도도 증가하고 있으며, 모바일 결제용 앱의 증가와 개인정보 보호에 대한 인식 확산이 이어지고 있어 사용자 계정 및 비밀번호, 그리고 결제 프로세스에 대한 더욱 높은 보안수준이 필요하게 될 것이다.

[그림 2-18]에서 보는 바와 같이 북미 및 유럽 지역 사용자 중 2/3의 응답자는 모바일 보안을 '매우 중요' 또는 '중요'한 것으로 생각한다고 답했으며, 중요하지 않다고 응답한 비중은 5.6%에 불과했다. 이는 해당 지역 내 스마트 모바일 기기 및 업무용 앱의 높은 보급률, 그리고 개인정보 보호에 대한 높은 인식이 반영된 것이다.

[그림 2-19]는 한 모바일 보안제품 제조사의 모바일 백신 소프트웨어에 대한 해외 소비자들의 피드백을 도표로 나타낸 것이다. 2009년 6월부터 2010년 동월까지 전체 모바일 보안문제의 2/3은 아시아 지역에서 발생했으며, 아프리카, 중동, 그리고 유럽 지역이 순서대로 그

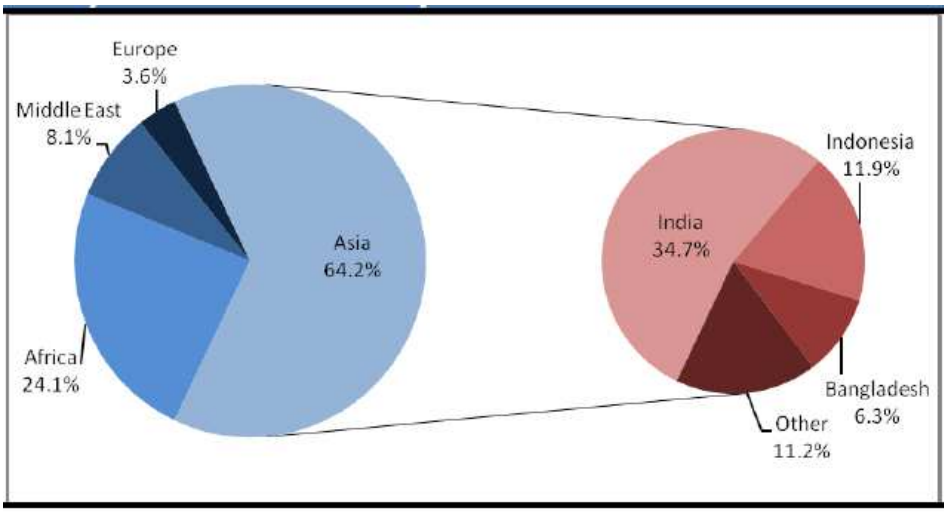
뒤를 이었다. 백신 문제에 대한 피드백을 제공한 64.2%의 아시아 지역 사용자 중 34.7%는 인도 지역 사용자였고, 인도네시아와 방글라데시 사용자가 각각 11.9%와 6.3%로 뒤를 이었다. 이로써 아시아와 아프리카가 비교적 심각한 수준의 모바일 보안문제를 겪고 있는 것으로 결론지을 수 있으며, 이들 지역을 향후 모바일 보안제품 공급자가 보안 서비스를 제공 기회를 창출할 수 있는 핵심 지역으로 볼 수 있다.

[그림 2-18] 북미 및 유럽지역 모바일 전화 및 앱 사용자들의 모바일 보안의 중요성에 대한 인식



모바일 보안제품에 대한 글로벌 보급률 분석 결과, 해당 분야 시장은 제품 수명주기 측면에서 도입기에 있다. 현재 해커들의 주요 관심영역은 여전히 PC 부문에 머물러있으나, 향후 스마트 모바일 인프라와 모바일 인터넷 SW의 보편화가 진행되면 특히 모바일 결제 등을 비롯한 모바일 휴대전화로 취급 가능한 정보로 취할 수 있는 이득을 노린 해커들이 모바일 영역으로 눈길을 돌리게 될 것이다. 그러한 시나리오에서는 모바일 바이러스 등을 위시한 각종 보안문제가 터져나올 가능성이 높기 때문에 모바일 보안제품 시장의 빠른 성장이 촉발될 것이다.

[그림 2-19] 중국산 모바일 보안제품에 대한 해외사용자들의 피드백



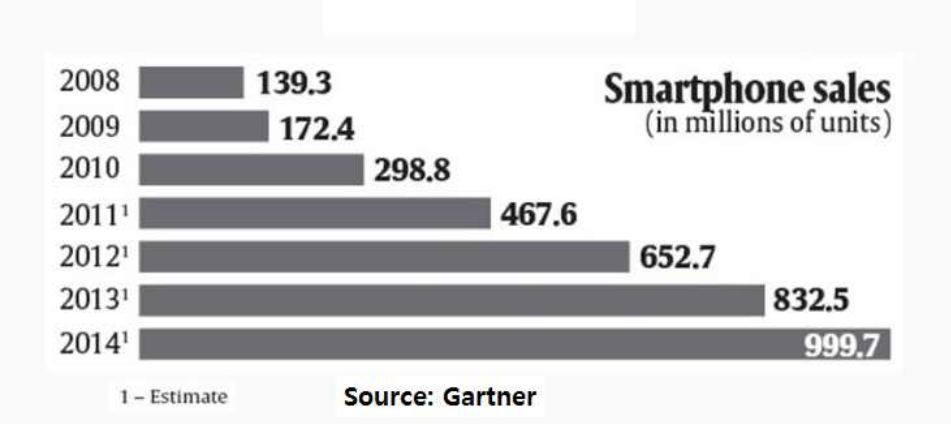
다양한 글로벌 보안 SW 선도업체들은 모바일 보안제품을 이미 출시했거나 곧 출시할 계획임을 밝힌 바 있으며, 해당 업체들의 모바일 분야에 대한 관심과 참여는 모바일 보안제품 시장의 형성과 중요성 부각에 큰 영향을 주고 있다. 그러나 현 시점에서 모바일 보안제품 시장의 주도권을 쥐고 있는 제조사는 존재하지 않는다. 모바일 보안제품 제조사는 크게 PC용 백신 SW 선도업체(Symantec, McAfee, Kaspersky, Trend Micro, Kingsoft, Rising 등)와 모바일 보안제품 제조업체(Bluefire, SMobile, NetQin 등)의 두 부류로 구분해볼 수 있다.

3. 글로벌 모바일 보안 시장 예측

먼저 글로벌 모바일 보안시장 동향을 살펴보면, 스마트폰이 주도하는모바일 기기 보급 확대에 따라 모바일 보안시장도 급격한 성장세를 보여줄 것으로 이 분야의 시장조사 권위기관들은 예측했다. 시장조사기관인 Gartner에 따르면 2011년 전 세계 스마트폰 판매대수는 4억6760만대로 예상되고 있다. 이는 2008년의 1억 3930만 대보다 3배 이상 증가한 수치이며, 2010년과 비교해도 56% 이상 늘어난 수치이

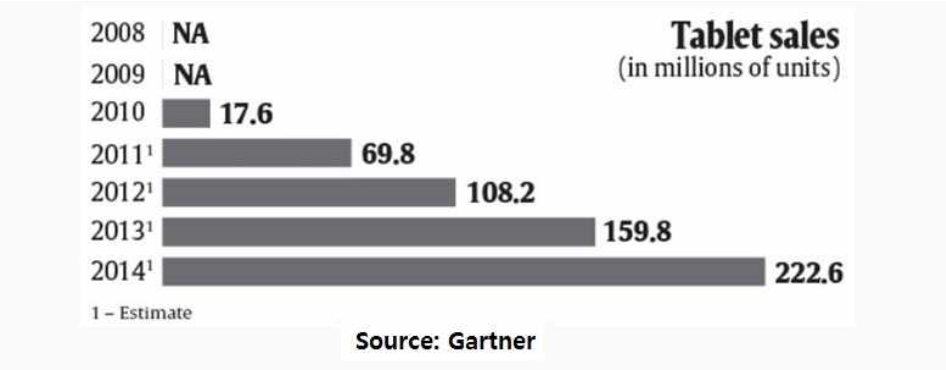
다. 또한 2014년에는 9억 9970만대로 판매대수가 늘어 스마트폰의 보급은 급격히 확대되는 추세임은 누구도 부인할 수 있는 현상이다.

[그림 2-20] 전세계 스마트폰 판매량 예측(단위 백만대)



한편, 2011년 전 세계 태블릿PC 판매량은 6360만 대로 예상되고 있다. 이는 2010년의 1760만대에서 무려 261.4%나 증가한 수치이다. 또한 2015년에는 3억 2630만 대로 판매대수가 늘어 수년간 태블릿PC 시장은 급격히 성장할 전망임을 보여주고 있다.

[그림 2-21] 전세계 태블릿PC 판매량 예측(단위 백만대)



[그림 2-22] 전세계 태블릿PC OS별 판매량 예측(단위 백만대)

Worldwide Sales of Media Tablets to End Users by OS (Thousands of Units)

OS	2010	2011	2012	2015
Android	2,512	11,020	22,875	116,444
iOS	14,685	46,697	69,025	148,674
MeeGo	179	476	490	197
Microsoft	0	0	4,348	34,435
QNX	0	3,016	6,274	26,123
WebOS	0	2,053	0	0
Other Operating Systems	235	375	467	431
Total Market	**17,610**	**63,637**	**103,479**	**326,304**

Source: Gartner

이상과 같은 스마트폰과 태블릿PC의 보급이 폭발적으로 확대되면서 모바일 보안시장도 급격한 성장세를 보여줄 것으로 예측되고 있다. 시장조사기관인 IDC에 따르면 2015년 전 세계 모바일 보안시장은 190억 달러 규모로 2010년의 4억700만 달러에서 비약적인 성장을 기록할 것으로 전망되고 있다. 이중 DLP (Data Loss Prevention)와 Encryption을 포함한 Mobile IPC (Information Protection and Control), MIAM (Mobile Identity and Access Management), MSVM (Mobile Security and Vulnerability Management), Mobile Threat Management, Mobile VPN(Virtual Private Network) 등이 2010년부터 2015년 사이에 연간 평균 30% 이상의 성장률을 보일 것으로 예측되었다. 아래 [그림 2-23]은 IDC가 매출액 기준으로 예측한 전세계 모바일 보안 시장규모와 성장 성장 추이를 보여주고 있다.

이와 함께 전세계 주요 통신기업과 IT 기업들도 폭발적으로 성장할 모바일 보안시장 선점 위해 적극적 행보를 할 것으로 보도되고 있다. 여기에는 보안업체뿐만 아니라 이동통신사도 가세하고 있다. Symantec, McAfee, Trend Micro, Webroot 등이 모바일 기기당 연평균 30달러 선에서 Anti-Virus Protection, 백업 데이터 저장, 분실 또는 도

난당한 모바일 기기 위치추적, 웹브라우징 모니터링, 원격으로 모바일 기기에 저장된 데이터 삭제 서비스 등을 제공하고 있거나 할 예정으로 있다. 또한 미국 주요 이동통신업체인 AT & T는 최근 Juniper Networks와 협력관계를 체결해 비즈니스와 개인용 모바일 보안 플랫폼을 개발한다고 발표하였다. 이렇게 개발된 소프트웨어는 올해 말부터 AT & T 네트워크를 통해 유료로 다운로드받을 수 있게 될 예정이다.

[그림 2-23] 모바일 보안 제품군별 전세계 판매액 예측
(단위 백만USD)

Mobile Security Product Sales Forecast(Million USD)

	2010	2011	2012	2013	2014	2015	2010–2015 CAGR (%)
Mobile threat management	99.1	179.2	280.2	350.1	415.2	470.4	36.5
Mobile IPC (encryption + DLP)	78.2	140.1	238.3	334.9	405.1	460.2	42.5
Mobile VPN	125.2	190.2	259.6	330.1	385.2	431.2	28.1
MIAM	43.8	69.9	117.1	164.2	194.8	225.7	38.8
MSVM	40.2	65.7	94.8	129.1	160.5	190.2	36.5
MOS	20.4	29.7	44.1	53.9	64.9	75.1	29.8
Total	406.9	674.8	1,034.10	1,362.30	1,625.70	1,852.80	35.4

Source: International Data Corporation(IDC)

AT & T Chief Security Officer인 Ed Amoroso는 모바일 기기가 24시간 이용할 수 있는 필수품으로 부상하고 있어 모바일 보안에 대한 인식이 높아지고 있다고 언급하였으다. 그러나 보안업체 Symantec이 실시한 설문조사에 따르면 24개국의 1만 2704명 중 16%만이 최신 모바일 보안소프트웨어를 모바일 기기에 설치했으며 10%가 모바일 관련 사이버 범죄의 피해를 본 적이 있다고 대답해 모바일 보안 소프트웨어 시장의 성장 가능성이 높은 것을 엿볼 수 있다.

시장조사기관 IDC의 리서치 애널리스트인 Stacy Crook은 모바일 기기의 확산 및 모바일 보안에 대한 인식이 높아지면서 기기당 연간 30달러에 이르는 금액을 모바일 보안비로 지출하게 되는 소비자들이 증가할 것으로 전망했다. 이에 따라 관련 보안업체는 새로운 수익원으로 인해 호황을 누릴 것으로 Stacy Crook은 예상했다. 또한 최근 유명 할리우드 배우인 스칼렛 요한슨의 스마트폰이 해킹당하는 등 모바일기기 해킹사례가 언론에 보도되면서 모바일 기기 해킹에 대한 소비자들의 우려가 커짐지고 있다고 보도된 사례도 있다.

이상의 모바일 보안시장에 대한 예측과 의견을 종합해보면, 모바일 기기의 보급이 확대되고 관련 모바일 애플리케이션의 수가 급격히 증가하면서 모바일 보안에 대한 관심이 증가할 것으로 예상되는 가운데, 모바일 보안업체들과 이동통신사 등이 관련 보안 소프트웨어를 출시했거나 출시할 계획에 있으며 향후 모바일 보안시장에 진출하는 업체 수가 더욱 증가할 것으로 예상된다.

제3장 모바일 보안 핵심기술과 경쟁력

제1절 정보보호 기술과 모바일 보안 기술

1. 정보보호기술의 분류와 발전

모바일 보안기술은 앞 장에서의 산업에 대한 정의와 분류 때와 마찬가지로 결국 정보보호 기술의 일부분으로 파악될 수 있기 때문에 단순하게 먼저 일반적인 정보보호 기술에 대한 고찰에서 시작할 수 있다. 정보보호 기술은 그 관점과 목적에 따라 매우 다양하게 분류될 수 있지만 여기서는 우리나라의 모바일 보안 기술의 경쟁력 확보와 개발 전략이라는 관점에서 최근에 정부차원에서 체계적으로 분류를 시도한 2010년 『한국산업기술평가관리원』 발표한 지식정보보안 연구개발전략의 지식정보보안 중장기 기술로드맵의 핵심기술 분류안을 채택하였다. 지식정보보안 중장기 기술로드맵과 핵심기술 분류안은 각각 다음 <표 3-1>과 <표 3-2>에 보여지고 있다.

지식경제부는 안전하고 안심할 수 있는 지식정보사회 구현과 2015년 국제 경쟁력을 갖춘 세계 일류 보안기술 확보를 목표로 R&D를 추진할 계획이다. 이를 위해 기술성·시장성·시급성·공공성을고려하여 국가경쟁력 제고 및 안전성을 확보할 수 있는전략 분야를 발굴하여 집중적으로 개발하고 정보보호 제품에 대한 국제적인 품질인증 기술을 확보하며 해외공동연구 활성화를 통해 선진국과의 기술격차를 해소하고자 한다. 또한 정보보호 분야의 급변하는 기술환경에 대응하고 중장기 기술개발 목표를 달성하기 위한 이정표를 담은 중장기 기술개발 로드맵 (2010 ~ 2015)을 수립하였다(<표 3-1>). 특히 시장과 제품, 기술과 서비스의 연계를 강화해 정보보호 정책 추진의 일관성을 유지하고 새로운 기회를 조기에 획득할 수 있는발판을 마련하였다.

<표 3-1> 정보보안기술 개발 로드맵

구분		2010	2011	2012	2013	2014	2015
서비스	공통기반보안	온라인 기반형 정보보안 기반 서비스		온/오프라인 연계형 정보보안 기반 서비스		지능형 정보보안 기반 서비스	
	네트워크/시스템 보안	가용성/생존성/신뢰성이 강한 네트워크 인프라					
	응용/서비스 보안	유무선 응용 보안 서비스	미디어 복합형 응용보안 서비스			지능형 응용보안 서비스	
	물리보안	영상기반 보안 서비스	보안 상황 인지 서비스			지능형 자율 대응 서비스	
	융합보안	컴포넌트형 융합보안 서비스			통합형 융합보안 서비스		
제품/솔루션	공통기반보안	온라인 ID 관리 시스템	온/오프라인 연계형 ID관리 시스템			지능형 ID관리 시스템	
	네트워크/시스템 보안	40G L3/L7 DDoS 공격 대응 시스템			지능형 L3/L7 통합 DDoS 공격 대응 시스템		
	응용/서비스 보안				시멘틱/모바일 웹보안 2.0 시스템		
	물리보안		프라이버시 보장형 DVR 시스템		실시간 신변/산업위험 대응 시스템		
	융합보안		차량통신용 착탈식 보안 모듈			차량 위험상황 인지 솔루션	
핵심기술	공통기반보안	온라인 신원 확인	온/오프라인 연계형 신원확인/지불		상황인지기반 신원확인/지불		
	네트워크/시스템 보안	실시간 네트워크/웹기반 DDoS공격 통합대응		지능화된 DDoS/PDoS 공격 패킷 탐지/차단			
	응용/서비스 보안		개방형 시멘틱/모바일 웹 보안				
	물리보안	프라이버시 보장형 영상보안		신변/산업 위험 실시간 인지/대응		상황인지 기반 능동형 통합보안 관제	
	융합보안	차량통신 보안 모듈/칩셋			차량센서 보안 플랫폼		

[출처 : 한국산업기술평가관리원, 지식정보보안R&D발전전략, 2010년]

인터넷을 안전하게 보호하기 위한 기술에는 크게 응용서비스 보호기술과 네트워크 보안기술이 있다. 응용서비스 보호기술에는 최근 전자상거래의 확산에 따라 전자서명, 키관리, 인증서비스를 제공하기 위한 암호화 기술, 인증기술, 전자서명, PKI, WPKI 등이있다.

<표 3-2> 정보보안 핵심기술의 분류

소분류	핵심요소기술	정의
공통 기반 보안	암호 알고리즘	암호화(encryption)와 복호화(decryption)에 사용되는 알고리즘을 의미하며, 대칭키 알고리즘(DES,3DES,AES), 공개키알고리즘(RSA,ELGamal), 타원곡선 암호알고리즘, 일방향 해쉬함수(MD5,SHA) 등 존재
	암호 프로토콜	시스템 내부의 데이터 뿐만 아니라 네트워크 상에서 시스템 간에 전송되는 데이터를 보호하기 위해, 암호기술을 이용하여 메시지를 교환하는 기술
	양자암호	빛의 양자역학적 특성을 이용한 암호화 통신 방법으로, 수신자/송신자 이외의 제3자가 key를 알아내는 것이 이론적으로 불가능한 기술
	인증 인프라	시스템 및 네트워크 접근을 제어할 수 있는 기술로, 식별(Identification), 인증(Authentication), 권한부여(Authorization) 등이 존재
	부채널 공격 대응	암호화에 사용된 키를 찾기 위해 암호 알고리즘의 이론적 취약점이 아닌 암호화 과정에서 누설되는 타이밍 정보, 전력소모, 전자파 신호 등을 이용하는 물리적인 공격에 대한 대응 기술
	개인정보보호	개인정보를 보호하고 유출을 방지하며 안전한 서비스를 이용하게 하는 모든 기술 (※ 개인정보 : 개인에 관한 정보 및 해당 정보에 포함되어 있는 성명, 주민등록번호 등 개인을 식별할 수 있는 정보를 의미)
네트워크 및 시스템 보안	네트워크 침입 대응	네트워크 인프라에 대한 침해와 네트워크 노드의 비정상적인 동작으로 인한 마비현상을 방지하고 응용서비스 연속성을 제공하기 위한 기술(Firewall, IDS,IPS, ESM, VPN 등)
	악성코드 대응	'악성코드'란 컴퓨터에 악영향을 끼칠 수 있는 실행 가능한 코드로, 자기 복제 능력과 감염 대상 유무에 따라 바이러스, 웜, 트로이목마 등으로 분류되며, 이에 대한 대응 기술
	보안운영체계	일반적인 컴퓨터 운영체계의 커널(Kernel)에 부가적인 보안기능을 추가한 운영체제로, 커널의 취약성 보완 및 엑세스 기능, 권한 부여 등이 가능한 운영체계
	디지털 포렌식	정보기기에 내장된 디지털자료를 근거로 발생한 사실 관계를 증명하는 보안기술로, 자료의 수집/보관/분석/보고에 이르는 일련의 절차와 방법에 관련된 기술
	보안칩	하드웨어 플랫폼에 보안 기능을 탑재하여 컴퓨터 메모리에 저장되어 있는 다양한 애플리케이션을 다양한 공격으로부터 안전하게 보호하는 칩
	접속보안	로그인시 필요한 데이터를 암호화하여 전송하는 방식으로 네트워크상에서 발생될 수 있는 다양한 위협으로부터 데이터를 보호하는 기술
	보안성 평가	보안 평가기준과 보안 평가제도로 구분 - 보안 평가기준 : 정보제품의 보안위협 대응능력 등 보안성 정도를 평가하는 기준 - 보안 평가제도 : 평가기준을 기반으로 평가 주체/절차/결과관리 등에 관한 규정
서비스 및 응용 보안	지식콘텐츠 보안	콘텐츠의 무단 사용 금지 및 제공자의 권리와 이익을 보호해주는 기술 및 서비스로, DRM, UCC보안, CAS 등 포함
	응용 서비스 보안	웹, VoIP/MoIP, 전자상거래, 전자투표, 이메일 등의 각종 응용 서비스에 사용되는 보안기술

시스템들로는 취약성 분석 시스템 (Vulnerability Scanner), 바이러스백신, AAA(Authentication, Authorization & Accounting) 서버 등이 있다. 네트워크 보안기술은 네트워크 인프라에 대한 침해와 네트워크 노드의 비정상적인 동작으로 인한 마비현상을 방지하고 응용서비스의 연속성을 제공하는 수단이다. 이러한 시스템에는 침입차단 시스템(Firewall), 침입탐지 시스템(Intrusion Detection System :IDS), 가상사설망(VPN) 시스템 등이있다.

그러나 이러한 단순 기능 형태의 현재 네트워크 보안시스템으로는 개별 호스트나 지역망 레벨에서 단편적인 침해에 대응하는 역할을 수행할 뿐이다. 또한 유해 주소 차단과 알려진 취약점 공격 탐지 등 제한적인 보안 기능만을 가지고 있어서 다양하고 복잡해지는 최근의 네트워크 공격에 대해서 효과적인 대응이 어렵다. 따라서 보다 안전하고 신뢰성 있는 인터넷을 구축하기 위해서는 우선적으로 광역 네트워크를 기반으로하는 정보보호 기술의 채택이 필요하며 나아가 인터넷을 시작으로 BcN, USN (Ubiquitous Sensor Network), Ad hoc 네트워크 등 미래 네트워크의 진화 추세에 따른 단계적인 네트워크 보안 기술의 개발이 필요하다. 이로 인해 최근 네트워크 보안시스템의 시판 경향은 개별 보안제품에서 통합 보안의 형태로 변화하고 있으며, 속도와 보안성의 크기가 동시에 보장되는 형태의 제품들이 본격적으로 시판되고 있다

2. 정보보안 기술의 연구개발 현황과 모바일 보안기술의 등장

(1) 국내의 지식정보 보안기술 개발

① 기술개발수준

기술개발 분야를 <표 3-2>와 같이 5대 소분류, 23개 핵심 요소기술로 분류하고 이를 대상으로 기술수준을 분석하였다. 기술수준 조사 결과 지식정보보안 기술 분야에서 전반적으로 미국이 최고 기술보유국이라는 응답이 가장 많았으며(87%), 한국·일본이 그 다음으로 소수

의 응답을 보인 것으로 조사되었다. 이를 소분류로 나누어 분석한 결과 모든 소분류에 있어 미국의 기술수준이 압도적으로 높은 가운데 '융합보안'을 제외한 기술은 유럽이 일본보다 높은 것으로 조사되었다. 우리나라의 경우'서비스 및 응용보안'에 있어 미국에 이어 높은 기술수준을 보유하고 있으며'공통기반보안'및'물리보안'에 있어 높은 수준을 80% 이상 보유하고 있는 것으로 조사 되었다. 기술격차 기간에서는'서비스 및 응용보안'의 격차기간이 가장 짧고'네트워크및시스템 보안'의 기술격차 기간이 가장 긴 것으로 조사되었다.

② 지식경제부의 기술개발계획

지식경제부는 융합산업 보안시장 창출을 위한 원천 보안기술 개발을 목표로

- 어린이 보호구역 터널 공공시설 등에서 안전 위협을 인지할 수 있는 객체정보 획득 휴먼 검출·식별 위험상황인지 기술
- 산업기술 유출방지를 위한 초소형 USB·플래쉬 메모리 탐지기술
- 내부정보 유출방지 및 악성코드 차단을 위한 20 Gbps급 데이터 유출 방지 기술
- 스마트 디바이스용 경량·저전력 암호구현기술
- 모바일 기기용 안전성·사용성 강화를 위한 인증·암호 원천기술

등 신규과제 R&D 계획을 수립하였다. 또한 기존에 수행해 오던 계속과제의 지속적인 수행을 통하여 산업적 파급 효과가 큰 보안기술을 확보하고 보안시장 활성화에 기여하기 위하여

- 개인 신변 안전보장을 위한 영상 보안 기술
- 자동차·의료 IT 융합산업을 위한 융합보안기술
- IT 및 법률 환경 트렌드에 부합하는 실시간 현장분석 포렌식 기술
- 편리하고 안전한 모바일 인증·지불·신원확인을 위한 스마트 지

갑 기술

- 산업기밀 보안을 위한 물리공간과 사이버 공간 연동을 통한 침입 탐지·대응기술

에 대한 R&D를 추진할 계획이다.

<표 3-3> 지식경제부의 정보보안 기술개발 계획

구분	과 제 명	연구기간
계속	실시간 분석을 위한 디지털 포렌식 기술 개발	'10~'13
	모바일ID 보안 및 프라이버시를 위한 스마트 지갑 기술 개발	'10~'12
	산업시설 정보자산 보호용 공간연동 침입 탐지 및 대응 기술 개발	'10~'12
	Car-헬스케어 보안 기술개발	'10~'13
	개인신변 안전보장을 위한 영상보안 기술개발	'10~'12
'11년 신규	사람에 의한 안전위협의 실시간 인지를 위한 능동형 영상보안 서비스용 원거리 (CCTV 주간환경 5m 이상) 사람 식별 및 검색 원천기술 개발	'11~'13
	산업기술 유출방지를 위한 초소형(1.5cm X 1.5cm) 전자소자 탐지 기술개발	'11~'13
	유무선융합(Fixed Mobile Convergence) 환경에서의 가상화 보안 기술을 이용한 스마트폰 데이터 보안기술과 20Gbps급 하드웨어기반 네트워크 내부정보유출방지 원천기술 개발	'11~'13
	모바일 환경하에서 모바일 인증을 위한 직관적이며 사용하기 편하고 안전한 인간-컴퓨터 상호작용(HCI)기반 Usable Security 원천기술 개발	'11~'14
	스마트 디바이스용 칩(ARM7/9/11, UICC 등)에 최적화된 암호(ARIA, SEED, KCDSA 등)의 국가 인증 모듈 및 배포 체계 개발	'11~'14

③ 방송통신위원회의 기술개발 계획

방송통신위원회는 유무선 인프라·단말·서비스의 안전성을 보장하기 위한 핵심 원천기술 개발을 목표로

- 모바일 인터넷망의 안전성 확보를 위한 3G 모바일 구간의 공격 트래픽 조기 탐지 및 다양한 트래픽에 대한 선별적 차단 기술
- 다양한 모바일 클라우드 환경에 적용가능한 범용성 모바일 클라우드 사용자·단말 통합인증 및 권한관리 기술
- 스마트 디바이스 종류에 관계없이 보호된 영상의 공유·이동·소

비가 가능한 스마트 영상보호기술

- 스마트 워크용 단말의 서비스 이용 안전성과 편리성 제공을 위해 개인정보 유출 및 비인가 사용자의 불법접근 등과 같은 침해확산 방지를 위한 보안기술 개발

등을 중심으로 신규과제의 R&D 계획을 수립하였다. 또한 기존에 수행해 오던 계속 과제의 지속적인 수행을 통하여

- 부채널 공격에 의한 u-디바이스 복제 및 비밀정보 유출 우려를 해소하기 위한 부채널 공격방지 기술
- 대규모 인터넷 환경에서의 불건전·유해 멀티미디어 콘텐츠 분석·차단기술
- DDoS(분산서비스거부 Distribute Denial of Service attack) 공격을 조기에 탐지하고 대응하기 위한 대용량 40G) DDoS 대응 시스템
- 사이버 공격에 체계적이고 신속하게 대응하기 위한 실시간 보안정보 공유 기반 통합 보안 제어 기술
- 다양한 사이버 공격으로 인한 피해확산을 억제하고 사전예방을 위한 지능형 악성코드 자동분석 기술 등의 R&D를 추진할 계획이다.

<표 3-4> 방송통신위원회의 정보보안 기술개발 계획

구분	과 제 명	연구기간
계속	상용 양자암호 통신시스템을 위한 요소 기술 개발	'08~'11
	부채널 공격방지 원천 기술 및 안전성 검증 기술 개발	'09~'12
	유해 멀티미디어 콘텐츠 분석/차단 기술 개발	'09~'11
	분산서비스거부(DDoS) 공격 대응 기술 개발	'09~'11
	전역적 협력기반의 통합보안제어 시스템 개발	'10~'12
	지능형 악성코드 자동 분석 및 경유/유포지 탐지 기술 개발	'10~'13
'11년 신규	3G 모바일 인터넷 망 침해방지 기술 개발	'11~'13
	모바일 클라우드 통합 인증 및 권한관리 기술 개발	'11~'13

④ 국내민간기업의 정보보호 원천기술 개발

정보보호 기업의 기술개발과 관련해 자체 기술연구소 및 전담부서 운영현황을 조사한 결과 기업부설 연구소를 운영하는 기업은 53.5%, 연구개발 전담 부서를 운영하는 기업은 29.0%로 나타났다. 연구소 및 전담 부서에서 종사하는 인원을 살펴 보면 기업부설 연구소를 운영하고 있는 기업의 종사자는 10인 60인 미만의 종사자를 가진 기업이 53개의 기업으로 가장 많고 연구개발 전담 부서를 운영하고 있는 기업 역시 10인 60인미만의 종사자를 가진 기업이 가장 많았다.

<표 3-5> 기술연구 전담인력 운영 현황

(단위 : 명)

구분	운영현황		종사자 기준			
	비율(%)	업체수	10인 미만	60인 미만	100인 미만	100인 이상
기업부설연구소 운영	53.5	107	22	53	18	14
연구개발전담부서 운영	29.0	40	10	15	7	8
운영하지 않음	26.5	53	31	19	1	2

[출처 : 한국인터넷진흥원, 2010 국내 정보보안산업 실태조사, 2010년 12월]

정보보호 기업의 연도별 기술개발 투자액 현황 및 향후 전망을 조사한 결과 2009년도 기술 연구개발비 투자액 규모가 있는 업체는 모두 144개로 업체당 투자액은 평균 588.8 백만원이며 기술도입비 투자액 규모는 평균 44.38 백만원 각종 인증획득 비용투자액 규모는 평균 26.01 백만원으로 나타났다. 2010년도 기술 연구개발비 투자액이 있는 업체는 모두 133개로 업체당 평균 584.48 백만원이며 기술도입비 투자액 규모는 총 41개 업체에서 평균 105.64백만원 각종 인증 획득 비용 투자액 규모는 총 71개 업체에서 평균 54.27 백만원을 투자한것으로나타났다. 향후 2011 년도 기술 연구개발비 투자액 규모는 총 108개 업체에서 평균 802.87 백만원이며 기술 도입비 투자액 규모는 총 39개 업체에서 평균 100.52 백만원 각종 인증획득 비용투자액 규모는 총 52개 업체에서 평균 80.77 백만원을 투자할 것으로 조사되었다.

<표 3-6> 기술개발 투자액 현황

(단위 : 백만원)

구분	2009년도		2010년도		2011년도(전망)	
	업체수(개)	평균	업체수(개)	평균	업체수(개)	평균
기술연구 개발비	144	588.80	133	584.48	108	802.87
기술 도입비	144	44.38	41	105.64	39	100.52
각종인증획득비용	144	26.01	71	54.27	52	80.77
매출대비 비율	144	11.5%	116	12.7%	93	12.8%

[출처 : 한국인터넷진흥원, 2010 국내 정보보안산업 실태조사, 2010년 12월]

정보보안 기업이 기술개발시 겪는 애로사항을 조사한 결과 '기술개발인력 확보 및 유지'가 82.7%의 비율을 보이며 가장 큰 애로사항으로 지적되었다. 다음으로는'자금조달'이 50.2%, '기술정보 부족 및 획득 곤란'이 9.3%,'신기술의 짧은 수명주기'가 1.0%,'연구설비 기자재 부족'이 4.3%의 순으로 조사되었다.

<표 3-7> 기술개발시 애로사항

구분	비율(%)
기술개발인력 확보 및 유지	82.7
자금조달	50.2
기술 정보 부족 및 획득 곤란	19.3
신기술의 짧은 수명주기	11.0
연구 설비기자재 부족	4.3
기타	0.6

[출처 : 한국인터넷진흥원, 2010 국내 정보보안산업 실태조사, 2010년 12월]

(2) 모바일 보안기술의 등장과 진화

현재 3세대 이동통신의 발달과 이를 활용한 풍부한 모바일 애플리케이션을 제공하고 있는 스마트폰의 성장으로 인해 인터넷 서비스 이용률이 테스크탑에서 모바일 단말로 전환되고 있다. 모바일 서비스를 지원하는 모바일 단말의 진화 과정을 살펴보면 1세대에 아날로그 방식의 음성 통화를 목적으로 한 기본적인 폰 기능에서 2세대에 디지털 방식으로 전환되면서 음성 통화 및 SMS와 같은 소량의 데이터 전송이 가능한 데이터 서비스를 지원하였다. 현재 지원하고 있는 3세대 이동 통신은 음성, 데이터 및 영상 등을 고속으로 주고받을 수 있는 멀티미디어 통신 서비스를 지원하고 있다.

3세대 이동통신 기술을 지원하는 모바일 단말은 일반폰과 스마트폰으로 구분할 수 있고, 하드웨어적인 면에서 유사한 특징을 가지고 있다. 하지만, 모바일 서비스를 지원하는 범용 OS 및 모바일 애플리케이션을 포함하는 소프트웨어 플랫폼은 많은 차이가 있다. 최근 스마트폰의 등장과 성장에 따라 모바일 소프트웨어 플랫폼에 대한 관심이 증가하고 있다. 또한, 아이폰과 앱스토어의 성공은 스마트폰에서 사용될 애플리케이션에 대한 관심을 한층 끌어올리고 있다. 하지만, 개방형 플랫폼 증가와 앱스토어의 등장으로 인하여 범용 OS를 채택하고 있는 모바일 단말은 모바일 악성코드의 제작을 용이하게 만들고, 제작된 모바일 악성코드는 범용 OS로 인해 이식성이 높기 때문에 모바일 공격의 피해가 증가할 것으로 예상된다.

스마트 모바일 기기의 발전은 다채로운 모바일 앱 SW 개발을 위한 필수 환경을 제공하며, 모바일 앱의 보안환경은 시간이 갈수록 다양한 도전과 위협에 직면하고 있다. 따라서 향후 더욱 지능화 되고 다양한 형태로 변형될 수 있는 악성 코드 정보 유출, 불법 과금, 부정 사용등과 같은 보안위협으로부터 모바일 단말 사용자를 보호하고, 활성화되고 있는 모바일 서비스 환경에 대한 안전성, 무결성,가용성 및 신뢰성을 제공하기 위한 모바일 서비스 보안기술 개발이 요구된다.

3. 모바일 보안 분야와 이슈

(1) Wireless Communication 일반과 보안이슈

Wireless Communication은 이동성을 보장한다는 점에서 미래 인터넷에서 가장 중요한 부분이다. 예컨대 산업 현장에서 정보수집과 폐루프 제어(Closed-loop Control) 등을 무선통신으로 할 수있어 기업경영에도움이 될 수있다. 미래로 다가갈수록 무선통신의 비중은 폭발적으로 늘어날 것이다. 하지만 인터넷의 출현이후 지난 20여년간 유선에 대한 기술개발이 지속적으로 이루어져 지금처럼 안전한 네트워크로서 역할올 하는 것처럼 미래 인터넷에서 무선환경이 유선환경처럼 제공되려면 해결해야 할 보안 이슈가 산재해 보인다.

우선 다양한 네트워크 인터페이스의 혼재로 인해 복잡성이 증가할 것이다. 모바일 환경이 예상보다 빨리 도래하여 스마트폰처럼 무선통신이 가능한 디바이스들이 폭발적으로 증가하였다. 스마트 오피스 등이 가능해지고 지정된 한 곳에서 인터넷을 접속할 필요가 없어졌다. 하지만 무선통신의 환경은 유선보다 훨씬 취약하다. 우선 무선 디바이스들의 연산능력이 일반 PC들 보다낮아 완벽한 보안기능올 첨가할 수없어 피해가 발생할 가능성이 높다. 특히 모바일 디바이스를 가진 불특정 다수가 피해를 입어 예컨대 공공서비스가 비정상적으로 중단될 경우 대규모 사회적 비용의 발생도 불가피할 것이다. 무선 단말기 확대로 정보유출, 위변조. USN에 대한 보안위협도 크게 증가할 것이다.

또한 Wireless Communication은 무선 주파수 대역폭 문제와 배터리 문제 등으로 시스템 자원을 보호하는데 어려움이 따를 수 있다. 최근에 크로스-레이어(Cross-Layer) 공격에 무선 네트워크가 취약한 것으로 나타나고 있다. RF와 관련해 분산된 신호(Dispersed Signal)를 해커가 감지하면 어떤 식으로든 통신올 방해해 트래픽올 증가시키고 다른 네트워크에 접속할 때 이를 방해할 가능성도 높다.

이와같이 미래에는 무선으로 많은 서비스와 정보가 이동할 것임에도 불구하고 유선 수준의 보안위협에 대한 대비는 많이 부족하다. 그러므로 무선환경에 기반올 문 미래 인터넷 환경은 문제가 유발되었올 경우 현재보다 사회적 비용이 많이 발생할 것이다.

하지만 무선 환경의 문제는 유선통신에 비해 기술적으로 완벽히 보안문제를 해결할 수 없다는 사실이다. 최대한 피해를 최소화 하는 것이 중요하며 적절한 암호화와 인증 기술올 활용하면 상당한 수준으로 해결이 가능하다. 특히 모바일 디바이스를 위한 경량 SSL 기술은 매우 중요하다. 전송 송출 수준을 감소시키거나 이에 해당하는 기술을 개발하는 것도 중요하고. 주파수 도약(Frequency Hopping Radio) 기술을 사용하여 전파 방해나 다중경로 페이딩(Multi-path Fading)을 방지하는 것도 하나의 방법이다.

또 무결성 기술을 개발하여 내외부의 공격에서 신뢰할 만한 무선 네트워크를 구축하여야한다. 이미 개발된 보안 프로토콜을 무선 단말 및 센서 등에 적용하는 것도 보안문제를 상당 부분 해결할 수 있는 방법이 될 것이다.

관련 분야의 기술개발 비용은 상대적으로 높을 것이다. 특화된 연동기기가 증가될 것으로 예상됨에 따라 각기 기술 적용 비용의 증가가 예상된다. 하지만 기술적인 측면보다는 오히려 관리적인 측면이 더 중요할 수도 있다.

관련 법규나 또는 정책적 지원과 관련해서 Rogue AP, 보안이 취약하게 설정된 퍼블릭 AP 등에 대한 운영관리 의무 제공 및 접속 규제가 우선적으로 필요하다. Wireless Communication 보안이슈는 기술적인 문제만으로는 해결이 불가능하므로 무선기기 전파관련(출력 등) 규제가 중요하다. 예컨대 제조업체와 서비스 제공자들에 보안에 대한 일정 책임올 부가하는 제도적 장치도 고려해 볼 필요가 있다. 모든 국민의 무선 단말기와 공공 및 민간환경에 설치된 통신장비에 보안기능을 의무화하는 것도 고려할 만하다. 한편 짝Wireless Communication 보안이슈는 영향도와 발생 가능성이 대단히 높고 비

용에 비해 해결 가능성은 크지 않을 것으로 나타나 시급하나 대비책이 필요한 것임을 알 수 있다.

(2) USN 보안이슈

지금까지 RFID 또는USN 관련 보안이슈는 업계와 전문가들 사이에서 막연히 제기돼 왔다. 하지만 미래 인터넷 환경에서는 센서의 증가로 인해 개인정보보호 차원에서 보안문제가 지금보다 크게 대두될 것이다. 사회 인프라 전반에 걸쳐 다양한 이종간 기기의 사용, 근거리 무선통신 기술이 탑재된 장비들의 사용이 늘어나게 됨에 따라 USN 보안이슈가 발생할 가능성이 높다.

미래에는 1인 1단말이 아닌 1인 N개의 센서를 사용할 것으로 보인다. 따라서 하나의 센서가 잘못될 경우 N개의 센서 모두 위험에 빠질 가능성이 높다. 특히RFID 등USN 네트워크 시스템에서는 정보도청, 개인정보 침해는 물론 태그 위·변조, DDoS 공격을 통한 시스템 마비 등 문제가 발생할 가능성이 크다. 이런정보도청 등을 통해 한 사람이 다수의 RFID 태그를 보유할 경우 태그 정보를 통해 1차정보를 유출하거나 개인의 소득, 질병유무, 취미성향등에 대한 프로파일링이 가능해 질 수 있다. 예컨대 공공기관에서 제공하는 서비스의 경우 개인에게 매우 중요한 정보가 많이 포함되어 있는데 이러한 정보가 센서등을 통해 노출될 경우 국가공권력에 의한 개인정보 침해가 발생할 수 있다고 정부는 지적하고 있다. 이와 함께 악의적 공격자가 태그와 단말기 간 통신에서 서비스거부 공격(DoS)을 발생시켜 시스템을 공격할 경우 시스템을 적용한 물류등 시스템 전체의 중단을 가져올 수 있는 것으로 보고 있다. 또 태그 위·변조와 전파방해 등을 이용해 절도 등의 범죄가 발생할 수 있는 것으로 나타났으며 위급상황에 이용되는 센서 정보가 위·변조되면 인명에 심각한 문제를 가져올 수 있는 것으로 분석되었다. 이는 센서 등이 제한된 저장 및 연산능력, 한정된 배터리 내구성으로 인해 다양한 암호화와 관련된 보안설정이 어렵기 때문이다. 특히 배터리나 동력 등이 쉽게 방전되며, 혹독한 자연 환경

속에서 쉽게 파손될 가능성도 있다. 정보노출, 복제, 스푸핑, 정보오인, 유령노드의 가능성도 있다.

실례로 보안카메라, 키보드, 주차 센서, RFID의 도입, 스마트 폰 등을 이용해 공격자는 침실이나 욕실과 같은 사적인 공간까지 침투하여 개인정보를 습득할 수 있다. 컴퓨터의 웹갬올 통해 우리의 인터넷 관심사롤 추적했던PC 스파이웨어 같은 형태가 나올 수 있다. 또 바코드를 잘못 판독하여 슈퍼마켓 등에서 이중요금을 과금하거나, RFID를 악성코드에 감염시켜 퍼트릴 수도 있다.

가장 위험한 위협은 데이터베이스에 저장된 정보들이 공격자에 의해 조작되어 통화내용이나 의료기록, 신용기록, 범죄기록, 위치정보 등이 노출되거나 조작될 수 있다는 데 있다, 이러한 사례는 사회적으로 큰 혼란을 야기할 수 있다.

기술적으로 다른 보안이슈에 비해 해결가능성이 전혀 없는 것은 아니다, 예컨대 가짜 센서(Rogue Sensors)의 차단, 센서 데이터의 기밀성 및 무결성 확보, 경량화된 암호 프로토콜의 이용, RFID 내의 정보유출올 방지하는 기술, RFID 리더와 태그간의 통신보호 기술, 가짜 리더 및 가짜 태그 탐지기술 등을 이용할 경우 기술적인 해결도 상당부분 가능하다, 또 보호) 및 차단기 등의 추가적인 기능과 결합하거나 자동화 솔루션을 통해 기기 스스로 진화하여 자체적으로 보안을 통제할 수 있도록 하는 것도 미래에 기대할 방법이 될 수 있다.

하지만 개인정보 유출과 관련해 보안기술이 개발되어도 편의성 제약으로 인해 채택올 하지않올 가능성도 높다, 또 전파간섭으로 인해 발생하는 문제는 해결하기가 어렵고, 소형 기기의 특성상 전력량, 메모리 크기, 연산능력, 통신속도 등의 제약사항도 있다.

이와 관련한 법적 규제로는 센서 노드 및 RFID 태그의 설치 장소와 관리 등에 대한 규제, 제조업체, 서비스 제공자들에게 보안에 대한 책임을 부가하는 제도적 장치, 타 기기에 대한 동작 방해를 방지하고 규제 및 개인정보를 수집할 수 있는센서 및 장비가 설치될 수 있는 환경적 조건올 가져야 하며 설치시 의무 사항 등에 대한 규정이 필요하다,

USN 보안이슈와 관련하여 본연구에서는 영향도와 사회적 비용, 발생가능성 등은 상대적으로 다른 보안이슈에 비해 낮은 것으로 나타났다. 이러한 결과는 다른 보안이슈에 비해 USN보안이슈가 상대적으로 보안상의 문제점을 일으킬 가능성이 적다는 것을 의미한다, 하지만 소형기기를 감염시켜 악성코드를 유포시키는 기술이 더욱 발전한다면 매우 큰 문제가 될 수 있음으로 주의가 필요할 것이다,

(3) 클라우드 컴퓨팅 보안이슈

클라우드 컴퓨팅 보안이슈는 미래 인터넷 환경에서 가장 중요한 핵심이슈 중의 하나이다, 내 정보를 가상의 공간에 저장하고 언제, 어디서든지 필요한 시간과 장소에 구애받지 않고 제공하는 클라우트 컴퓨팅 기술은 지금과는 다른 차원의 새로운 경험의 기회를 제공할 것이다. 최근 클라우드 서비스에는 사용자가 증가하고 사용량도 많아지고 있다, 클라우드 컴퓨팅 보안이슈는 사용자와 사용량이 많을수록 문제발생시 비용이 크다,

미래 인터넷에서 인터넷의 속도 증가는 클라우드 컴퓨팅 의존도를 높일 것으로 예상된다. 인터넷에 접속하는 속도가 증가되면 클라우드 서비스를 사용하는데 느끼는 불편함이 감소함으로 더욱 많은 소비자나 기업이 클라우드 서비스를 통해 시간과 비용을 절약할 수 있게 된다. 이러한 패러다임의 변화에 따라 보안문제도 주목을 받을 것이다. 예를 들면 Google이나Amazon과 같은 기업이 가지고 있는 하나의 서버에 데이터를 집중할 경우 이러한 사이트에 공격이 발생하면 수많은 개인정보가 유출되어 사회적으로 큰 파장이 예상된다. 기업 역시 광범위한 개인정보 침해가 발생하는 것은 물론이거니와 기업의 자원이나 전략 또는 업무상 비밀이 경쟁사에 노출될 경우 계산할 수 없는 손실이 발생할 수 있다.

특히 기업 단위의 공격은 매우 주의할 필요가 있다. 기업의 입장에서는 IT기술을 통해 시간과 비용을 절약할 수 있기 때문에 클라우드 컴퓨팅 활용도가 높아질 것이다. 하지만 해커 입장에서는 개인단위처럼 볼특정한 다수보다는 이름있는 기업단위 공격 타겟이 단일화

됨에 따라 클라우드에 대해 공격하고자 하는 빈도가 증가할 것이다. 실제로 클라우드 서비스에 대한 가장 큰 우려는 보안문제였다.

한편 일부에서는 클라우드 환경에서 보안이슈를 중앙에서 통제가 능하므로 상대적으로 안전하다고도 주장한다. 하지만 대부분의 경우 안전하다고 생각하는 중앙에서 통제하는 하나의 사이트 또는 서비스가 문제를 야기할 경우 파장은 쉽게 예상할 수 없다.

그러면 과연 기술적으로 해결이 가능한가? 가상화 및 클라우드 컴퓨팅에 대한 기술은 꾸준히 연구하고 있어 어느 정도는 해결될 것으로 보인다. 현재가 기술활성화 단계라면 향후에는 보안기술들이 더욱 많이 연구될 것으로 보인다.

다양한 보안기술을 개발하려는 시도가 예상되는 가운데 클라우드 컴퓨팅 서비스 제공자들에서 보안은 클라우드 서비스의 핵심과제로 인식하게 만드는 것이 매우 중요하다. 업체들이 수익만을 고려하지 않고 실시간으로 모니터링 시스템을 갖추고], 데이터에 대한 암호화 및 백업 작업을 게을리 하지 않는다면 위협은 많이 감소할 것이다. e-Discovery기술, 대용량 패킷처리가 가능한 침입탐지기술(IDS), 개인인증, 개인정보보호, 접근통제를 이용한 기업 데이터 보호기술 등도 더욱 개발할 필요가 있다. 클라우드 컴퓨팅 보안이슈의 발생가능성을 국내와 해외로 비교해서 살펴보면 국내보다는 해외의 클라우드 컴퓨팅 서비스 보급률이 훨씬 높기 때문에(예컨대, 아마존 서비스) 해외에서 먼저 문제가 발생할 소지가 높다. 그러므로 대부분의 서비스는 외국회사가 중심이 될 것으로 보이며 국내에서는 외국에서 문제가 발생하고 어느 정도 보안문제가 해결된 후 본격적으로 활성화 될 가능성이 높다.

클라우드 컴퓨팅 보안이슈를 위한 정책적 대안으로는 데이터 위탁관리, 디지털 포렌식(Digital Forensic), 자료 와 운영에 대한 권한 분리 등에 대한 기준이 우선적으로 마련되어야 한다. 또 나의 데이터가 외국회사에 고스란히 저장됨으로 이를 관리하고 책임소재를 분명히 하기위해 국제적 데이터를 관리하고 법률적 제도를 정비하는 등 정책적

기준을 찾아야 한다. 특히 프라이빗 클리우드와 달리 공용으로 이용되는 퍼블릭 클라우드는 법적 규제가 반드시 필요하다.

(4) 모바일 오픈마켓과 콘텐츠 보안이슈

미래 인터넷에서는 모바일을 통한 다양한 비즈니스 모델이 새로운 수익원으로 각광받을 것이다. 기업들은 모바일 광고를 강화하고 신규 모바일 서비스를 제공하며, 개인들은 모바일을 통해 자신의 삶을 스마트하게 최적화시켜 생활할 것이다. 하지만 이러한 변화는 모바일 오픈마켓과 콘텐츠의 보안이슈를 수반한다. 특히 이동통신 서비스 사업자 중심의 공급자 중심 시장에서 사용자가 다양한 콘텐츠를 이용할 수 있는 플랫폼을 제공하는 사용자 중심 시장으로 패러다임이 이동함에 따라 모바일 오픈마켓과 콘텐츠 관련 보안이슈는 더욱 중요하게 부각될 것이다.

예컨대 최근 스마트폰의 활성화로 정보공유가 활발히 일어나고 있다. 스마트폰을 통해 모바일로 업무를 하고 앱과 콘텐츠를 다운받아 사용하고 있다. 이러한 모바일 시장의 확대는 경제적 측면에서는 새로운 기회를 제공하고 개인에게 새로운 경험을 제공한다는 측면에서는 긍정적이나 보안문제에는 취약할 수 있다. 대개 비즈니스 모델과 보안은 반비례 하는 경향이 있다.

모바일 마켓은 모바일 앱과 콘텐츠를개발자가 공급하고, 사용자가 구매할 수 있는 형태로 새로운 유통구조를 만들어 내어, 스마트폰 등 모바일 기기를 통해 새로운 사업기회를 제공한다. 대표적인 모바일 마켓으로는 애플의 앱스토어와 구글의 안드로이드 마켓이 있으며, 국내의 경우, 에스케이텔레콤의 T-Store와 쇼스토어 등이 있다. 애플의 앱스토어의 경우 애플의 관리하에 에플이 제공하는 심사 기준에 따라 앱을 등록하는 등 폐쇄적 구조를 갖고 있으며 현재 약 30만개 이상의 앱이 등록된 것으로 알려져 있다. 구글의 안드로이드의 경우 애플과 달리 마켓을 열어 놓고 개입하지 않는 개방형 앱마켓 정책을 펴고 있다. 안드로이드 마켓의 경우 개발자는 누구나 등록이 가능하고 최소한의 검증도 이루어지지 않아 마켓자체가 악의적인 앱을 유포할 수

있는 곳으로 활용될 가능성이 높다. 따라서 우선 인가 받지 않은 앱과 보안상 결함이 포함되어 있는 앱이 유통될 경우 보안상의 문제가 야기될 가능성이 높다. 앱을 통한 악의적인 공격이 가능해져 악성코드가 확산된다면 따라서 문제는 심각해 진다. 실제 스마트폰 등 무선통신 단말의 사용확대가 악성 앱의 확산을 도와 개인정보 유출 및 공격에 단초를 제공할 가능성이 제기되고 있다. 또 다양한 스마트 디바이스를 이용한 콘텐츠의 확산이 성인물 등의 유해정보를 언제, 어디서나 유통할 수있도록 할 수 있으며 불법배포와 저작권문제로 확대될 수도 있다. 이 경우 개인에게 지적재산권 및 저작권침 해문제가 발생할 소지가 있다. 실제로 인터넷이 보급되면서 저작권 관련 문제가 많은 사회적 논란을 초래했다는 점을 고려하면, 향후 미래에도 사용이 편이성 증가에 비례하여 이러한 문제가 발생할 소지가 높다. 모바일 오픈마켓도 많은 사용자들이 접근함으로 보안문제가 발생할것이다.

이러한 문제를 해결하기 위해서는 우선 앱스토어 내의 검증을 강화하여야 한다. 앱스토어 운영자는 안전성이 확보된 코드를 이용한 앱을 유통시켜야 하며 보안에 허점이 있거나 불건전한 앱의 유통은 철저히 근절할 필요가 있다. 또 정보의 유출이나 공유에 대한 적절한 관리와 데이터에 대한 합법적인 권한에 대한 기술도 필요하다. 무선기기의 증가 및 기능 향상에 따른 상호인증 기술 및 안전한 코드 개발 기술도 필요하다.

현재 국내에서는 콘텐츠 공유에 대해서는 별다른 법적 조치나 대응이 없다. 콘텐츠 보안문제를 근본적으로 해결하는 것은 거의 불가능하고 개별적으로 막기가 매우 힘들기 때문에 적극적인 관심과 대응이 필요한 실정이다. 다만 DRM 등의 기술을 강화하는 등의 조치는 필요하다.

앱과 관련해서는 해외업체의 경우 자체적인 운영체제 플랫품을 가지고 있어 자체적인 모바일 앱 검증이 가능함으로 모바일 오픈마켓 보안을 일정 수준으르 보장할 수 있으나 국내는 아직까지 많이 부족한 실정이다.

관련 규제로는 민간에서 각 플랫폼별 앱 개발 및 검수 가이드라인을 강력히 운영하여 과거 불법 소프트웨어 공유로 인해 소프트웨어 산업이 입었던 손해가 발생하지 않도록 해야 한다. 앱스토어 등에 대한 규제 및 정책적보완, 세금부과문제, 앱사업자에 대한 보안의무사항 준수 제도도 필요하다.

(5) Mobile Device 보안이슈

201 l0년11월 현재 약 30 여종의 스마트폰이 출시되면서 사용자가 500만명을 넘겼을 정도로 모바일 디바이스에 대한 관심과 증가의 폭이 급증하고 있다. 이러한 추세는 미래 인터넷환경에서는 더욱 폭발적으로 증가할 것으로 보이며 모바일 데이터 서비스가 활성화 되어 유선중심의 서비스 환경이 모바일 환경 중심으로 이동할 것으로 예측된다. 스마트폰으로 대변되는 모바일기기는 사용자 중심의 장치로 접근성이 좋고 젊은 층을 중심으로 빠르게 확산될 것이다. 기업들이 이러한 추세에 발맞춰 현재 무선 인터넷망을 확충하고 속도를 높이기 위해 차세대망을 준비하고 있다. 한편으로는 이러한 인프라를 기반으로 웹스토어 마켓 활성화와 모바일 결제 시장 확대를 위해 노력하고 있다.

하지만 모바일 디바이스는 분실, 악성코드 감염, 정보유출, 금전적 손실, 공격지 활용 등 여러 가지 위협요인을 가지고 있다. 아무래도 개인용컴퓨터에 비해 연산능력이나 전원 지구성 등 시스템의 완결성 측면에서 부족해 보안에 취약성을 크게 가지고 있다. 특히 악성 소프트웨어를 통한 공격에 노출될 가능성이 큰데 윈도우기반 모바일 기기나 안드로이드 기반의 스마트폰의 경우 검증되지 않은 앱을 위장하여 사용자의 주소록, 통화기록, 문자 메시지 등을 빼돌리는 등의 사고가 급증하고 있다. 탈옥한 다른 모바일 기기의 경우에도 Cydia등 블랙마켓을 통해 모바일 디바이스에 대한 보안사고가 발생할 가능성이 높다. 또 모바일 단말기의 경우 배터리의 수명의 한계 때문에 다양한 기능을 동시에 구동시키기가 어려워 보안을 등한시할 가능성이 높다. 또 모바일 기기 사용량이 많은 만큼 네트워크의 복잡성이 야기되어

문제발생시 피해액도 클 것으로 예상된다. 위치정보를 비롯한 개인정보의 유출 등도 쉽게 생각해 볼 수 있는 문제다.

그럼에도 불구하고 모바일 기기의 확산은 피할 수 없는 대세가 된 것 같다. 미래 인터넷은 이종간 다양한 디바이스가 이무리 많이 사용되더라도, 더 많은 기기가 촘촘히 연결되더라도 서비스 사용을 원활히 하도록 지원하는 환경이다. 따라서 미래 인터넷 환경에서 모바일 기기간에 보안이슈는 발생빈도가 상대적으로 높올 것이며 향후 3 ~ 5년내에 지금보다 심각성이 더 크게 발전할 것이다.

이러한 문제점을 해결하기 위해서는 네트워크 설계 단계부터 보안이슈를 고려하여 설계할 필요가 있다. 이동단말과 네트워크간 암호화 및 단말인증, 제어기술이 좋은 예이다. 또한 구표준으로 구동되는 대량의 단말기와 AP들에 대해 펌웨어 패치를 설치하면 상대적으로 적은 비용으로 이에 대한 대비를 할 수 있다. 한편 국내의 잘 갖추어진 IT 인프라가 모바일 환경에서 오히려 해가 될 수도 있다. 국내 무선인터넷 사용량은 세계1위 수준이다. 따라서 Home LAN에 보급된 IP폰, IP-TV, 셋탑 박스내 포함된 취약한 아이디와 패스워드들이 공격의 대상이 될 공산이 크다. 기술과 환경이 변하기 때문에 정책이나 규제의 변경은 반드시 필요하다. 스마트폰이나 태볼릿 PC 등 다양한 모바일 서비스에 대한 정책 및 규제도입이 절실하다.

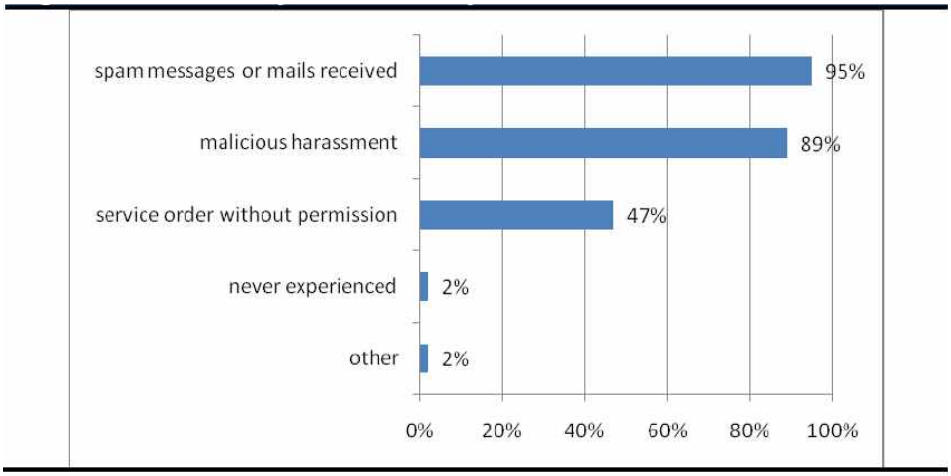
제2절 모바일 보안 기술에 대한 수요 현황 및 전망

1. 모바일 보안분야 주요 이슈

모바일 단말은 모바일 악성코드의 제작을 용이하게 만들고, 제작된 모바일 악성코드는 범용 OS로 인해 이식성이 높기 때문에 모바일 공격의 피해가 증가할 것으로 예상된다. 일례로 모바일 바이러스는 각 스마트폰에 탑재된 OS마다 각기 다른 유형의 피해를 입힐 가능성도 있으며, 스팸 메시지 역시 모바일 사용자들을 괴롭힐 여지가 충분하다. 서비스 주문용 앱은 금전적 손실을 입힐 수도 있으며, 음성통화

및 스팸 메시지를 이용한 각종 범법행위 및 모바일 기기의 분실 등도 개인정보 유출의 잠재적 위험성을 안고 있다. 모바일 보안 위험은 이미 심각한 사회문제를 야기하고 있어 각국 정부는 물론 통신사, 휴대전화 제조사들의 관심이 집중되고 있다. 다만 모바일 보안 취약성으로 인한 문제나 그 파급효과가 상대적으로 작은 까닭에 일반 사용자들의 모바일 보안에 대한 의식수준은 아직까지 높지 않은 수준이다.

[그림 3-1] 이동전화 사용자의 모바일 보안이슈



Source: Frost & Sullivan; Telephone survey result of 500 valid samples.

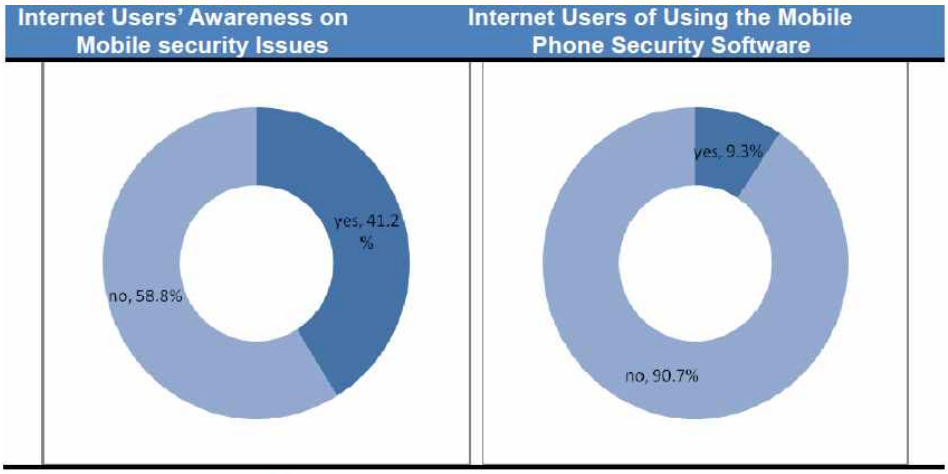
프로스트&설리번의 2010년 사용자 설문조사에 따르면 스팸 메시지 및 이메일, 개인정보 침해, 무단 유료서비스 결제 등이 모바일 보안의 주요 이슈인 것으로 나타났다.

모바일 인터넷 사용자를 대상으로 한 설문조사 결과 응답자의 41%만이 보안문제에 우려를 나타냈으며, 모바일 보안문제의 잠재적 폐해에 대해서는 아직까지 인식이 부족한 것으로 파악됐다. 스팸 메시지와 온라인 프라이버시 침해에 대한 사용자들의 수용성은 모바일 보안에 대한 인식 수준과 유사한 단계에 머물러있을 것으로 보인다. 모바일 보안문제에 대한 인식에 비해 모바일 보안용 SW를 실제 사용하는 사용자수는 더욱 적어, 고작 9.3%의 모바일 사용자만이 보안용 SW를 설치한 것으로 나타났다. 모바일 보안에 대한 일반 사용자들의

인식은 모바일 바이러스에 의한 공격이 일정 수위까지 도달하지 않는 한 크게 높아지지 않을 것으로 보이며, 모바일 보안 SW의 설치수요 증가 역시 인식 제고와 궤적을 같이할 것으로 전망된다.

2010년 한 해 동안 모바일 휴대전화 바이러스는 악성코드를 통한 개인정보 침해 및 무단결제 등의 영역을 포함해 모바일 기기에 설치된 시스템을 파괴하는 수준의 피해에서 민감한 개인정보(계정정보 및 암호 등)를 빼내거나 사용자 정보를 무단으로 업로드하는 단계까지 진화했다. 또한 모바일 휴대전화 바이러스의 유형도 다양화되는 모습을 보여 더욱 위험한 수준으로 발전했다. Netquin의 '클라우드 세이프' 데이터 분석센터가 제시한 통계에 따르면 2010년 한 해 약 2천 5백종의 모바일 바이러스가 발견되어 전년 대비 193%의 증가세를 보였고 감염된 모바일 휴대전화 수도 8백만대를 초과했으며, 변종 바이러스 역시 231종 이상 늘어난 것으로 파악됐다.

[그림 3-2] 인터넷 사용자의 모바일 보안이슈 인식

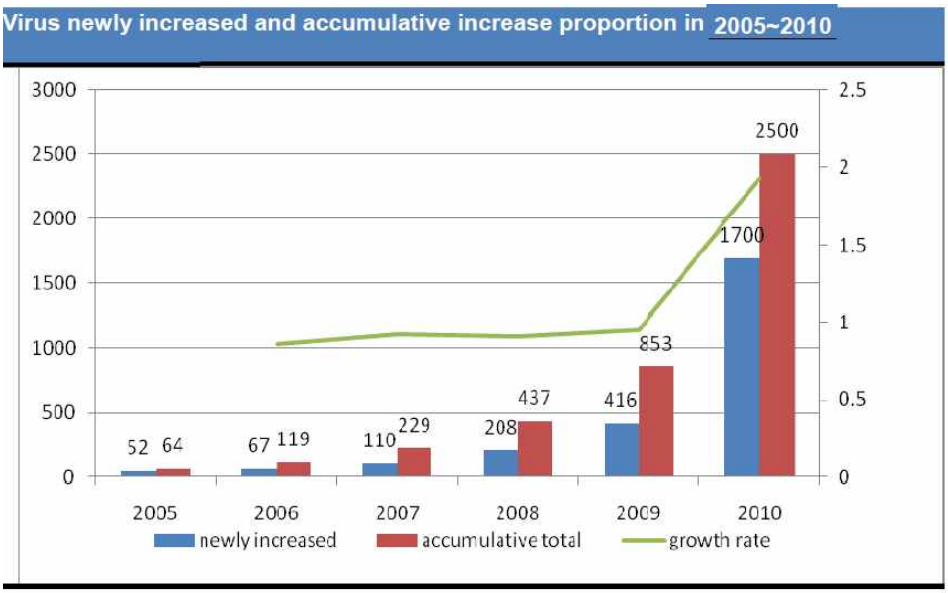


Source: Frost & Sullivan; Telephone survey result of 500 valid samples.

특히 중국 남동부 해안지역의 모바일 인터넷 환경이 급속도로 발전하면서 해당 지역 사용자들이 전체 사용자의 수적 증가를 견인했고, 이어진 모바일 앱의 폭발적인 성장에 따라 모바일 휴대전화 바이러스에 대한 위험도도 그만큼 증가했다. 일례로 2010년 '좀비'(11

월) 및 '휴대전화 스켈레톤' 모바일 바이러스 등의 출몰을 들 수 있으며, 상기 언급한 지역의 스마트폰 사용자들이 감염 피해를 입은 사례가 가장 많았다.

[그림 3-3] 모바일 바이러스 증가추세



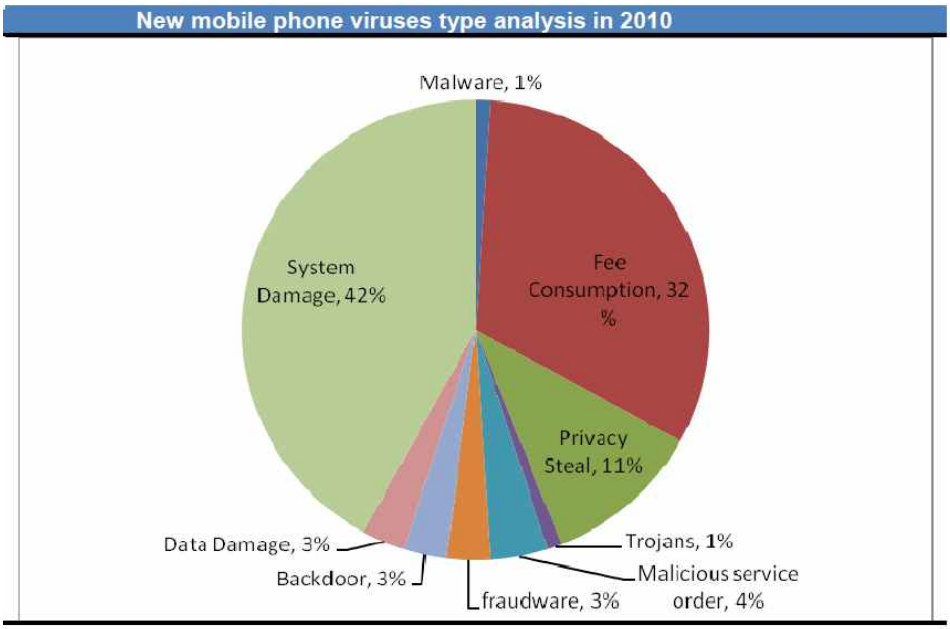
Source: Netqin "cloud safe" data analysis center

이어 프로스트&설리번에서는 악성 소프트웨어(모바일 바이러스 포함), 모바일 개인정보 침해 및 데이터 유출의 3대 영역에 걸쳐 모바일 휴대전화가 직면한 보안 위협요인을 상세히 분석했다.

향후에는 서비스 무단결제를 노리는 바이러스가 더욱 증가할 것으로 보인다. Netqin의 '클라우드 세이프' 데이터 분석센터 통계를 보면 2010년 (11월) 기준 모바일 휴대전화 정보유출 사고 가운데 968건이 모바일 바이러스를 통한 무단 현금결제(계좌정보 도용 454건, 바이러스 감염을 통한 구입대금 무단결제 514건)였으며 개인정보 불법유출이 334건, 트로이 바이러스 12건, 모바일 악성 소프트웨어 130건, 사기성 소프트웨어가 80건, 백도어 소프트웨어에 의한 모바일 데이터 파괴가 94건 등으로 집계됐다. 이외에도 모바일 휴대전화의 시스템을

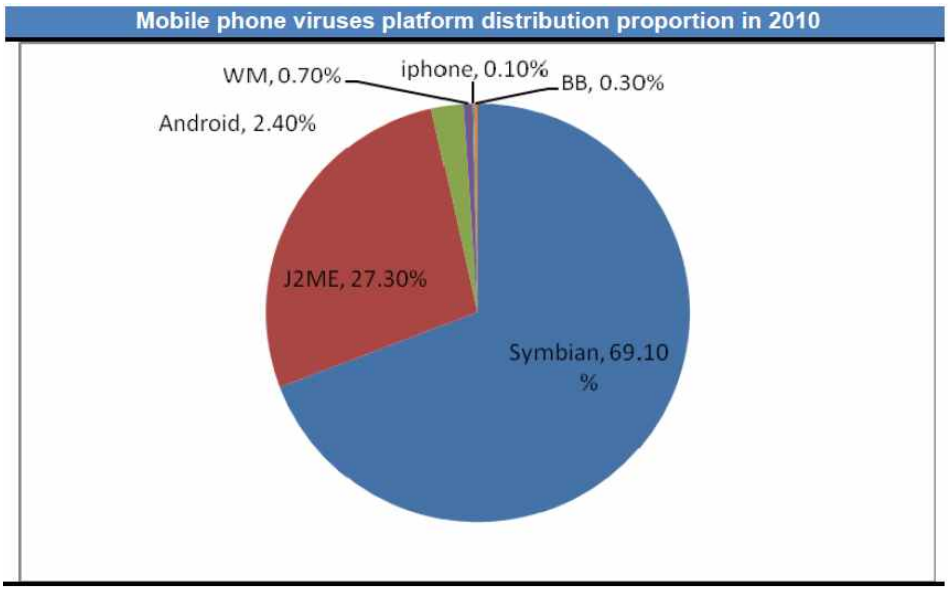
노린 바이러스 및 악성 소프트웨어가 각각 1,280종과 36종에 달했다.

[그림 3-4] 모바일폰 바이러스 타입



OS 가운데서는 안드로이드가 훨씬 빠른 속도로 증가했다. 2010년 전체 바이러스 통계자료를 보면 심비안 OS가 다수를 차지했으나, 2010년 말에는 안드로이드 앱 수가 2천만종을 넘어서며 약 25억회 이상의 누적 다운로드를 기록했다. 중국 내에서도 안드로이드 앱 개발 시장이 폭증 추세에 있어 JiFeng 네트워크 플랫폼에만 6천종 이상의 안드로이드 앱이 등록되어 있다. 그리고 현재 중국 시장 내 존재하는 안드로이드 앱 가운데 약 8%에는 무단 금융결제를 위한 악성 소프트웨어가 설치되어있는 것으로 파악된다. 저가형 스마트폰 시장이 점차 확대되면 그 비율도 늘어날 것으로 예상되며, 이러한 무단결제 앱의 경우 사용자가 해당 앱을 다운로드해 설치하는 과정에서 자동으로 실행되는 경우가 많아 사용자들의 피해는 커질 수밖에 없다.

[그림 3-5] 모바일폰 플랫폼별 바이러스



Source: Netqin "cloud safe" data analysis center

2. 스마트 단말기 보안 위협 요소

최근 스마트폰 이용 확산에 따라 시간과 장소에 구애 받지 않고 무선 인터넷을 활용하면서 기존 인터넷 사이트의 환경도 스마트폰 환경 변화에 맞춰 변화되고 있다. PC 환경에서 제공하는 인터넷 서비스가 스마트폰 환경으로 전환되면서 PC 환경의 보안 위협이 스마트폰 환경에서도 나타날 것으로 예상된다. 현재 인터넷 환경에서 PC를 대상으로 나타나는 다양한 유형의 공격은 백신, 방화벽 및 침입탐지 기술로 대응을 하고 있다. 이에 비해 스마트폰은 다양한 무선접속환경의 개방성, 휴대성, 저성능 등으로 기존 PC 환경의 보안 위협과 더불어 새로운 보안 위협에 노출되어 있다

(1) 스마트폰의 보안 특성

① 개방성

스마트폰은 일반폰보다 월등히 뛰어난 성능을 가지고 있으며 멀티미디어 처리도 우수하다. 하지만 최근에는 일반폰들의 사양이 스마트폰과 거의 차이 가 없을 정도로 개선되어 이를 기준으로 스마트폰과 일반폰을 구분하기는 어렵다. 스마트폰과 일반폰을 구별짓는 가장 큰 특성은 개방성이라 할 수 있다. 스 마트폰은 일반폰과는 다르게 무선 인터넷 및 외부 인 터페이스를 개방하여 제공하고 있다. 또한, 애플리케이션 개발시 시스템 자원의 사용을 위해 SDK를 이용하여 API 를 제공하고 있다. 스마트폰의 다양한 외부 인터페이스는 사용자에게 다양한 네트워크 서비스를 지원하고, 내부 API 인터페이스 제공은 개발자에게 편리한 개발환경을 제공한다 [4],[5]. 하지만 이를 보안적 측면에서 해석하면, 다양한 외부 인터페이스 제공은 악성코드 전파 경로의 다양성을 제공 하고, 내부 인터페이스는 악의적인 개발자에 의해 악성코드가 은닉된 모바일 애플리케이션 제작을 용이하게 만드는 취약점을 가지고 있다.

② 휴대성

스마트폰의 휴대편의성으로 인해 발생하는 분실/도난사고는 월평균 20만대에 이르고 있다. 스마트폰 분실/도난에 따른 직접적인 경제적 피해와 더불어 스마트폰에 저장된 개인정보 및 모바일 오피스를 지원하는 스마트폰의 특성으로 인한 기업의 중요 기밀정보의 유출은 심각한 사회문제를 야기시킬 수 있다. 이에 따라 스마트폰에 저장된 정보를 암호화하거나 분실/도난시 저장된 정보를 원격에서 소거하는 기술들이 등장하고 있다.

③ 저성능

스마트폰은 PC에 비해 저전력, 저성능 기기이다. 따라서, PC 환경에서 제공하는 보안 소프트웨어를 스마트폰에 적용하기에는 무리가 있다. PC 환경에서는 다양한 보안위협에 대응하기 위해서 지속적인 모

니터링을 통해 악성코드를 탐지해야 하지만 스마트폰은 전력 및 성능적 제한으로 인해 백신을 비롯한 보안 소프트웨어의 적용에 어려움이 있다.

(2) 모바일 악성 코드

모바일 악성코드는 스마트폰을 포함한 모바일 단말을 대상으로 정보유출, 단말파괴, 불법과금 등의 악의적인 행위를 수행하기 위한 악성 프로그램으로 정의할 수 있다. 모바일 악성코드는 모바일 단말의 성장과 더불어 규모면에서 빠르게 증가하고 있고, 위협요인도 다양화되고 있다. 모바일 악성코드가 증가하는 원인은 악의적인 목적을 가진 악성코드의 제작 및 유통이 가능한 개방형 단말기의 증가와 함께 블루투스, Wi-Fi와 USB 등 외부 접속의 다양화가 원인이라고 할 수 있다.

스마트폰 OS 보안수준의 경우, 아이폰 OS는 폐쇄형 OS로 안전하지만, 안드로이드 OS는 개방형 OS로 보안이 취약하다는 것이 일반적인 평가였다. 하지만 최근 PDF 취약점, 화면잠금 비밀번호 취약점 등 연이은 아이폰 OS 취약점이 알려지면서, 안전하게 설계된 폐쇄형 OS로 완벽한 애플리케이션 검증체계를 갖고 있어 보안솔루션이 필요 없다는 애플의 외침은 무색하게 됐다.

아이폰 OS는 애플사의 폐쇄적인 인증정책 때문에 지원하는 보안솔루션이 많지 않으며, 지원한다 하더라도 원격잠금 등의 기본적인 보안기능만을 제공하고 있어 보다 안전한 보안기능을 요구하는 업무에 사용하기에는 불안한 것이 사실이다. 반대로 안드로이드 OS 경우는 개방형 OS라서 '보안에 취약할 것이다 라는 인식이 있지만, 개방형 OS라는 태생적인 특성에 따라 애플리케이션 레벨의 보안기능은 물론 커널 레벨의 보안 기능까지 제공하는 다양한 보안솔루션이 등장, 전자결재 등 안전한 보안기능이 요구되는 업무에 사용하기에 적합한 방향으로 발전하고 있다. 다음의 <표 3-8>은 스마트폰 OS별 주요 악성코드 현황을 보여주고 있다.

<표 3-8> 스마트폰 OS별 악성코드 현황

스마트폰 OS	악성코드	설명
안드로이드	Android Spyware/SMSReplicator	문자 메시지를 사용자 몰래 실시간으로 특정 사용자에게 유출
	Android-Trojan/SmsSend	문자 메시지를 통한 과금 발생 유도, 다수 변종 출현
	Android Spyware/Snake	사용자의 GPS 정보를 특정 서버로 전송, 유료 어플인 GPS Spy TapSnake가 설치된 스마트폰 위치 확인 가능
	Android Spyware/Ewalls	스마트폰 내의 개인 및 단말기 정보를 수집해 특정 서버로 전송, 다수의 유사 프로그램 발생
	Geinimi	중국에서 발견, 개인정보를 특정 서버로 전송
윈도우 모바일	WinCE/TredDial	지적으로 국제전화를 무단 발신해 원치 않는 과금 발생
	WinCE/Duts	윈도우 모바일 최초의 바이러스, 실행파일 감염, 개념 증명 바이러스
아이폰	Ike worm	배경화면 변경, 아이폰 최초의 악성코드, 탈옥 기기에서 동작
	iPhone/Privacy.A	감염된 아이폰에서 무선랜을 접속하는 경우, 개인정보(문자메시지, 이메일 등)를 원격으로 전달
	Win-Trojan/Agent.535552.F	아이폰 탈옥 프로그램으로 위장한 정보유출형 악성코드, 구글토크, MSN 메신저, 야후 등의 서비스에 로그인할 때 ID와 패스워드 등의 계정 정보 유출

모바일 악성코드는 초기에 단순히 전파를 목적으로 하거나 단말의 기능적 동작을 마비시키는 형태에서 개인정보의 유출 및 금전적 이득을 목적으로 하는 형태로 변화되고 있다 지금까지 존재한 모바일 악성코드를 주요 활동별 특성을 반영하여 분류하면 5가지 형태로 구분할 수 있다.

① 단말 장애 유발형 악성코드

단말의 사용을 불가능하게 만들거나 장애를 유발하는 공격유형이다. 2004년에 발견된 Skulls가 단말의 기능을 마비시키는 단말 장애 유발형 악성코드의 한 예이다. 이 악성코드는 모든 메뉴 아이콘을 해골로 변경시키고 통화 이외의 부가기능을 사용할 수 없게 만든다. 2005년에 발견된 Locknut 악성코드는 단말의 일부 키 버튼을 고장내는 특성을 가지고 있다. 이외에도 전화의 송수신 기능을 마비시키는 Gavno가 등장하였다.

② 배터리 소모형 악성코드

단말의 전력을 지속적으로 소모시켜 배터리를 고갈시키는 공격유형이다. 2004년에 블루투스를 통해 전파되는 최초의 모바일 악성코드

인 Cabir가 대표적이다. Cabir는 단말의 침해를 유발하지 않는 대신 지속적으로 인근 단말의 블루투스를 스캐닝하고, 블루투스를 통해 악성코드를 전파하는 특징을 가지고 있다. 감염된 단말은 지속적인 스캐닝을 통해 배터리의 고갈 피해를 입게 된다.

③ 과금 유발형 악성코드

단말의 메시징 서비스나 전화 시도를 지속적으로 시도하여 과금을 발생시키는 공격 유형이다. 2006년 러시아에서 제작된 J2ME 플랫폼용 RedBrowser가 대표적인 사례로서 감염된 단말은 사용자도 모르게 불특정 다수에게 SMS를 전송함으로써 사용자에게 금전적 피해를 입히는 악성코드이다. 또한 중국에서 2008 년에 발견된 Kiazha 악성코드는 감염된 단말 화면에 사용자에게 돈을 요구하는 경고 메시지와 함께 단말 내에 저장된 문자메시지를 삭제한다.

④ 정보유출형 악성코드

감염된 단말의 정보나 사용자 정보를 외부로 유출시키는 공격 유형이다. 2008년 발견된 Infojack이 대표적인 예이다. 이 악성코드는 합법적인 애플리케이션이 단말에 다운로드될 때.cab 설치파일와 함께 포함되어 설치되고, 설치된 후 특정 웹서버에 접속하여 Infojack의 나머지 부분을 다운로드하여 재설치한다. 설치가 완료되면 단말의 보안 설정을 변경하고 단말의 시리얼 번호, OS, 설치된 애플리케이션 등 단말의 정보를 외부로 전송하여 2차 공격을 용이하게 한다. 사용자의 정보를 외부로 유출시키는 또 다른 악성코드로는 Flexispy, PBStealer가 있다. Flexispy는 스파이웨어 형태의 상용 악성코드로서 스마트폰의 전화기록, 문자메시지 내용을 특정 웹서버로 전송하는 기능을 가지고 있다.

⑤ 크로스 플랫폼형 악성코드

모바일 단말을 통해 PC를 감염시키는 공격 유형이다. 2005년에 발생된 Cardtrap.A가 최초의 크로스 플랫폼형 악성코드로서 폰의 메모리 카드에 윈도우 웜을 복사하여, 감염된 폰 메모리 카드를 PC에 장

착했을 때 autorun을 통해 PC를 자동으로 감염시켜 데이터를 삭제하거나 성능을 저하시킨다. 모바일 기기간의 확산이 아닌 모바일 기기에서 PC를 감염시킨다는 점에서 새로운 형태의 공격 유형이라 할 수 있다.

3. 모바일 보안 기술에 대한 수요

(1) 스마트폰 전자결제를 위한 보안기술

전자결제 등 보다 높은 수준의 보안이 요구되는 업무에는 애플리케이션 잠금 기능(비밀번호 확인 후 애플리케이션 실행)이나, 중요정보 암호화 등의 안전한 보안대책이 필요하다. 나아가 스마트폰 소유자가 기업의 중요정보를 무단으로 유출하는 것을 방지하기 위해 정보유출방지시스템(Data Leakage Prevention System)와 문서보안시스템(Digital Right Management System)과 같은 보안 강력한 보안기능이 요구된다. 또한 사용자 수가 많은 경우에는 스마트폰에 설치된 다양한 애플리케이션과 단말 하드웨어 자원, 그리고 각종 보안 솔루션들을 중앙에서 효율적으로 관리하기 위한 단말 관리와 통합 보안관리, 중앙관리 기능을 구현하는것이 필요하다.

스마트폰을 분실했을 경우, 원격잠금 기능을 설정하면 비인가자의 내부 업무시스템 접속 및 중요정보 접근을 차단할 수 있다. 하지만 원격잠금 기능은 네트워크 서비스를 이용해동작하므로 원격제어를 실행하기 전 비행모드를 설정하거나 USIM 카드를 제거하고 부팅하는 등 네트워크 서비스를 차단하는 경우에는 무용지물이 될 수 있다.

이러한 원인으로는 여러 가지가 존재하겠지만, 아직은 만족할 만한 보안 솔루션이 없다는 것과 보안 위협에 대한 심각성 인식이 부족, 모바일 오피스 구축시 보안대책 수립을 고민하지 않은 이유가 크다. 물론 최근에는 많은 보안업체들이 모바일 백신 등 다양한 보안솔루션을 내놓고 있다. 하지만 중요정보를 빼내거나, 통화 내역을 도청하는 악성코드, 위장 AP를 이용한 해킹, 테더링을 통한 우회 네트워크연결, 사내 메일의 웹메일 전달을 통한 중요 정보 유출 등 실제 발

생 가능한 위험에 대응할 수있는 만족할만한 보안솔루션은 아직없다.

(2) 스마트 오피스를 위한 보안기술

모바일 오피스의 도입 목적은 효율적인 업무 수행과 생산성 향상이다. 그러나 보안 문제가 발생한다면 그 효과는 퇴색될 수밖에 없으며, 기업의 존폐 위기에 놓일 수도 있는 심각한 사태에 직면할 수도 있다. 따라서 멀티 OS를 선택하기 전에 모바일 오피스를 통해 제공하고자 하는 서비스의 중요도와 요구되는 보안수준을 먼저 고려해야 한다.

높은 수준의 보안이 요구되는 업무는 모바일 오피스를 구현하기 이전 요구되는 보안수준 만족 여부를 먼저 검토해야 한다. 즉 구현하고자 하는 모바일 오피스에 대한 보안 대책을 수립하고, 보안 대책을 만족할 수 있는 OS를 선택하는 것이 바람직하다. 적용업무별로 다른 보안 요구사항 필요하다. 모바일 오피스에 필요한 보안 요구사항은 <표 3-9>와 같이 정의할 수 있다.

<표 3-9> 모바일 오피스 보안 요구 사항

분류	구분	기능	기능 상세
MDM 기능	단말관리	단말 정보수집	운영체제, 제조사, 통신사, 단말기 모델 등의 휴대폰 정보 수집
		디바이스 제어	와이파이/GPS/블루투스/카메라 등의 실행 통제
		단말 정책관리	네트워크 설정, 장소 및 보안설정, 응용 프로그램, 디스플레이 설정 등의 단말 관리
		승인관리	디바이스 사용 및 스토리지 중요정보 반출 승인, 리소스 사용 승인
		소프트웨어 관리	소프트웨어 설치 내역 모니터링, 소프트웨어 설치(배포 및 업데이트)관리
		원격 리소스 관리	실행 프로그램 관리 및 메모리 사용량, 저장공간, 배터리 사용량 등의 관리
	사용자 관리	단말/사용자 등록관리	인사DB연동 및 배치(Batch) 처리 및 일괄등록 및 개별등록 기능
		관리자 계정관리	정책/운영/로그 관리자로 권한 구분, 관리자의 IP 주소 접속제한
	이력관리	사용자 이력관리	사용자별 사용이력, IP정보, 위치정보, 애플리케이션 설치/삭제/사용 이력 등
		감사 관리	관리자 행위에 대한 이력관리
	공지 관리	공지사항 관리	개인별 /조직별/ 정책 대상별 공지 기능
분실/도난관리	단말 관리	원격 제어	단말 원격 잠금, 원격 잠금 해제, 중요 데이터 원격 삭제
		원격 조회	단말기 위치조회, USIM 변경 통제, 사이렌 경보, 비상 메시지 표시
		원격 감시	실시간 통화 감시, 통화 내역 조회, 배터리 잔량 확인 등 단말 감시
악성코드 대응	악성코드	악성코드 및	블랙리스트(도메인, 인증서) 기반 악성코드 검사
		위험 애플리케이션 검사	위험권한 리스트 기반 위험 애플리케이션 검사
	플랫폼 검사	시스템 취약점 검사	OS 및 각종 구성(configuration) 관련 취약점 검사

<표 3-9> (계속)

분류	구분	기능	기능 상세
정보유출 방지 및 데이터 보안	암호화	중요정보 암호화	사용자 지정, 애플리케이션 사용 중요정보, 주소록/통화기록/SMS내역 자동 암호화
			시큐어 폴더에 파일 이동 시 자동 암 · 복호화
		암 · 복호화	대칭키 AES, 대칭키 3DES, SEED, 해시 MD5, SHA1, SHA256 지원
		시큐어 스토리지	내부 메모리에 안전한 저장공간 제공
	모바일 DLP	정보유출방지	중요정보 식별 및 모니터링
			반출 승인처리 프로세스 제공 및 승인정책의 실시간 반영
		중요정보 접근 승인	보안정책에 따라 설정된 ACL 이외 애플리케이션의 중요정보 반출 행위 통제
			중요정보 접근 허용 애플리케이션(ACL)을 제외한 애플리케이션에 의한 중요정보 접근 제어
		디바이스 접근 승인	보안정책에 따라 차단된 디바이스(SD카드, 3G, 와이파이) 사용 통제
		정책관리 및 모니터링	중요정보 접근 정책(ACL) 설정 및 중요정보 접근 및 반출 현황 모니터링
	모바일 DRM	문서보안	모바일 게이트웨이와 스마트폰 사이 구간의 문서보안
		기존DRM 정책 연동	유선 환경의 보안문서를 무선 환경의 보안문서로 변환, 보안정책 연동(Mapping)
		모바일 문서 암호화	스마트폰에서 생성한 문서 암호화
			PC에서 생성한 문서가 스마트폰에 암호화 저장돼 네트워크 연결 없이 열람
	백업 및 복구	원격 백업	중앙 관리자를 통한 실시간 백업 또는 SMS 제어방식을 이용한 즉시 백업 실행
		다양한 백업 위치	시큐어 서버 또는 모바일 단말의 마이크로SD카드 등 백업 장소 선택 지원
		암호화 전송/저장	백업정보 암호화 전송 및 저장 및 Data 압축 및 암호화 지원
네트워크 보안	침해 대응	침입차단/방지	안바운드/아웃바운드 트래픽 통제
	채널 보안	VPN	기존 VPN 게이트웨이와 연동, 정보자산을 안전하게 이용 가능 하도록 지원
애플리케이션 보안	SSO	단일로그온	인사DB연동 및 배치(Batch) 처리, 단일 로그온으로 자원 접근
	애플리케이션 보안 관리	애플리케이션 실행통제	애플리케이션 다운로드 시 실시간 검사, 스케줄링 정기 검사, 실행시 악성 애플리케이션 실행 통제
	보안 정책 관리	보안 상태 분석	보안정책 및 보안상황과 연동돼 애플리케이션 및 디바이스 사용 통제
	중앙집중관리	정책관리 및 모니터링	각종 보안점검 정책 설정 및 패턴업데이트 및 보안점검 현황 모니터링
보안솔루션 자체 보호	난독화	리버스 엔지니어링	프로그램 난독화를 통한 리버스 엔지니어링
	애플리케이션 체크	애플리케이션 위/변조 방지	애플리케이션 위/변조 방지를 위한 서버, 단말간 위/변조 방지 체크
	강제 종료 및 삭제 방지	워치독(Watch Dog) 관리	프로세스 중지 및 보안모듈 임의 삭제 방지 기능
			보안모듈은 물론 중요 애플리케이션(프로세스) 등록 관리 기능 제공
통합 관리	중앙 관리 지원	정책관리/모니터링	단일 솔루션을 통한 기능 구현으로 중복 제거, 관리의 효율성 제공

현재 국내 모바일 오피스에 적용된 보안은 ID/패스워드 기반 인증, 24시간 주기의 인증 세션 관리, SSL이나 TSL을 이용한 인증정보의 암호화 전송, 문서를 서버에 저장하고 스트리밍 형태의 보기 기능만 제공하는 문서보안, 그리고 단말기의 분실 및 도난에 대응하기 위한 원격잠금과 주소록/SMS 내역 등을 삭제하는 원격 데이터 삭제, GPS 정보를 이용한 단말기 위치 조회 등이 대부분이다. 이는 기업의 중요업무를 스마트폰으로 처리하기에는 상당히 미흡한 수준이라고 말할 수

있다.

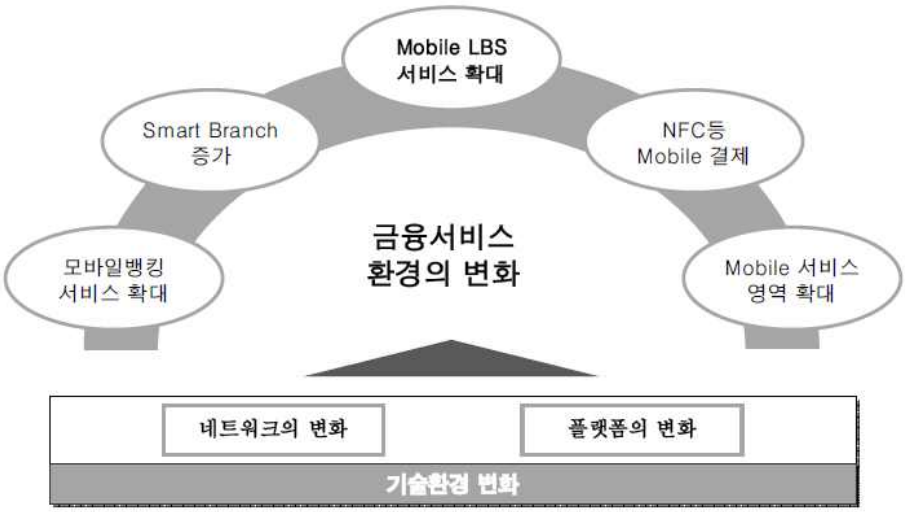
중요한 점은 모든 모바일 오피스 업무에 이러한 요구기능을 적용해야 하는 것은 아니며, 보안 대책 수립 결과에 따라 요구되는 보안 수준을 만족할 수 있도록 구현하면된다는 것이다. 예를 들어 사내메일 등 정보를 공유하는 수준의 업무시스템에는 '분실 및 도난 대응과 악성코드 감염 방지' 기능을, 전자결재 등 의사결정이나 중요 정보 접근이 가능한 시스템에는 '분실 및 도난 대응과 악성코드 감염 방지' 기능은 물론 '데이터 보호 및 네트워크 보호' 기능을 구현해야 한다. 모바일 오피스 요구기능에 대해 보다 자세히 살펴보면 분실 및 도난 대응에는 원격제어를 통한 단말잠금과 중요정보 삭제, 단말 위치조회와 백업 및 복구 기능이, 악성코드 감염 방지를 위해서는 안티바이러스(백신)와 미확인 또는 위험한 애플리케이션 및 프로그램 실행통제 기능이 요구된다.

데이터 보호에는 암호화와 시큐어 스토리지, DLP, DRM, 카메라와 미이크 제어 기능이, 네트워크 보호에는 스마트폰의 인바운드/아웃바운드 트래픽을 제어하는 방화벽과 안전한 네트워크 접속을 위한 가상사설망(VPN), 신뢰하지 않는 무선랜 AP를 통한 정보유출 및 스니핑 차단, 테더링 및 애드혹 서비스 통제, 봇넷(Botnet) 방지, 스팸 및 피싱 방지 기능 등이 요구된다. 단말관리(MDM)는 원격에서 모바일 기기를 관리할 수 있는 기능으르 펌웨어 업데이트 및 소프트웨어 배포, 버전관리, 단말 리소스 및 정책관리, 장애관리 등이 제공되어야 한다.

(3) 모바일 금융서비스를 위한 보안기술

금융서비스의 Mobiilliity화 확대는 금융기관의 비대면 채널 통합전략으로 연결되고 있으며 Mobile 시장은 네트워크와 플랫폼의 기술적 환경 변화를 기반으로 모바일뱅킹 서비스 확대, 스마트지점 증가, 모바일 LBS, 증강현실(AR) 등과 연계한 Mobile 결제서비스 확산, Mobile 서비스 영역확대 등으로 서비스 환경이 변화 양상을 보여주고 있다.

[그림 3-6] 금융서비스 환경의 변화



모바일 뱅킹의 활성화와 더불어 모바일 보안 관련 이슈들이 등장하고 있으며, 이에 따라 금융감독원 보안성 심의를 받지 못한 상황에서 스마트뱅킹 서비스 제공 및 방화벽, 백신프로그램, 키보드 보안 등 PC수준의 보안 프로그램 설치가 안되고 서비스 제공하고 있는 실정이며, 이에 감독당국 2011년 1월 가이드라인 마련했다.

<표 3-10> 스마트폰 전자금융 안전대책

부문	항목	대응 방안
전자금융거래 부문	• 다단계 가입자 확인 절차 마련. • 로그인시 사용자 인증강화. (공인인증 등) • PC 인터넷뱅킹과 유사한 보안수준 적용.	• 공인인증서 적용
기술적 침해대응 부문	• 금융거래 정보는 전 통신구간에 암호화적용. • 비밀번호등 중요입력 정보유출 및 변조 방지를 위한 입력정보 보호대책 마련. • 바이러스 등 악성코드 예방대책을 적용, 전자서명을 의무화하여 고객이 거래사실 부인 방지.	• PKI 암호화 적용 • 키보드보안 적용 • 백신 적용
취약점 모니터링 부문	• 스마트폰 관련 새로운 취약점을 신속히 인식하고 대응할 수 있는 모니터링체계 구축	• 관리, 감시 등의 정책적인 사항

자료:금융감독원

최근 하나은행의 아이폰 뱅킹 서비스가 감독당국의 보안성 심의를 통과하지 못한 상황에서 서둘러 출시되면서 고객 피해 우려가 높아지고 있다. 반면 전문가들은 PC와 비슷한 기능을 갖춘 스마트폰에도 공인인증서는 물론 방화벽과 백신프로그램, 키보드 보안 등 PC수준의보안 프로그램 설치를 의무화해야 한다는 의견이 꾸준히 제기되었다. 감독당국도 이미 내년 1월 중 이러한 내용을 골자로 하는 가이드라인을 마련할 예정이다.

국정감사에서 '2011년도 주요 정보통신기반시설 보호대책' 보고서에 따르면 전체 은행권의 침해예방 수준은 평균 78.3%였으며, 침해에 대응하는 수준은 73.1%로 나타났다. 국회 정무위원회의 한 의원이 23일 금융감독원 국정감사에서 공개한 '2011년도 주요 정보통신기반시설 보호대책' 보고서에 따르면 전체 은행권의침 해예방 수준은 평균 78.3%였으며, 침해에 대응하는 수준은 73.1%로 나타났다. 이 보고서에는 2010년도에 정보통신기반보호법 제9조(취약점의 분석·평가)에 의거해 각 은행들이 실시한 보안 취약점 분석결과 내용이 실려 있으며, 은행들의침 해예방 수준과 대응수준이 점수화되어 적시되어 있다.

"ㅅ"은행이 71.9%로 가장 낮은 수준의침해 예방 및 대응수준을 보였으며, 시중은행 중에는 "ㅎ"은행이 83.4%로 가장 취약했다. "ㅇ"은행(87.1%)과 "ㄱ"은행(80.3%)도 상대적으로 취약한 것으로 나타났다. 가장 높은 수준을 나타낸 곳은 또 다른 "ㅅ"은행(100%)이었으며, 또 다른 "ㅅ"은행(97.2%)과 또 다른 "ㅇ"은행(94.1%)은 상대적으로 높은 편이다. 또한 시중은행의 평균 침해 예방수준은 92.1%로 비교적 높았지만, 침해 대응수준은 81.9%로 비교적 낮게 나타났다.

국회정무위의 "ㅇ"의원은 "은행들이 금융결제원 ISAC이나 보안전문기관으로부터 받은 취약점 검사에서 총 2311개의취약 점이 발견됐다"면서 "특히 지방은행에서 모두 1191건의취약점이 발견됐다"고 지적했다. 그는 이어 "은행권이 여전히 취약한 보안체계를 갖고 있다"면서 "올해 유난히도 많았던 금융기관의해킹침 해 사고 및 전산사고 등이 이미 예견되었던 사건이었다"고 지적했다.

이에 따라 전자금융거래법 및 전자금융감독규정 개정안 변경의 필요성이 제기되고 있으며 금융위원회는“전자금융거래법과 전자금융감독규정”개정안 변경하여 금융회사 정보보호 강화를 위해 과거 감독기준으로 제시됐던 것을 규정으로 명문화하고 의무화하였다. 이 규정에 따르면 IT 부문 계획 제출을 전 금융회사로 확대하고 CEO의 책임 강화하여 금융회사 및 전자금융업자는 전자금융거래의 안정성과 신뢰성 확보를 위해 전자금융기반시설의 취약점 분석·평가 및 결과를 금융위원회에 보고해야 한다.

전자금융거래법 및 전자금융감독 규정에 따라 각 금융기관 및 IT 회사에서 법/제도적인 뒷받침을 위한 “보안 컨설팅”을 준비중이고, 이에 따라 보안인력 신규채용 및 보안인력의 업무범위가 확대될 것이다. 보안성 심의 및 보안시스템 도입, 취약점 분석 등에 따라 새로운 보안시스템 도입이 이루어지게 될 것이다.

<표 3-11> 전자금융거래법 및 전자금융감독규정 주요개정 내용

< 전자금융거래법과 전자금융감독규정 주요 개정 내용 >

법률 및 규정	개정안 내용	시행 후 영향
전자금융거래법 개정안	IT부문 계획 금융위 제출	IT부문 계획 제출 대상 확대
	기반시설 취약점 분석 보고	취약점 분석 보고 대상 및 범위 확대
	금감원 전자보조업자 조사	금융IT아웃소싱 및 금융SI 사업자 조사 가능
전자금융감독규정 개정안	IT인력 임직원 수 대비 5% 확보,정보보호인력 IT인력 대비 5% 확보(자체인력 절반 이상 확보)	IT SSC 시행한 금융그룹 계열 금융사 자체 인력 확보 시급(우리은행·경남은행·광주은행·하나대투증권·대한생명·한화손보 등)
	정보보호 예산, IT예산 대비 7%	예산 항목에 통신회선이용료, DR시스템 구축 비용 포함
	분석·설계 단계부터 보안 고려	프로젝트팀에 보안담당자 참여 여부가 기준
	정보시스템 감리 지침 작성·운영	내부자도 감리인 지정 가능, PMO도 인정

자료:금융위원회

제3절 모바일 보안 기술 연구개발 현황 및 전망

1. 국내 모바일 보안기술 연구개발

국내에서의 모바일 보안기술에 대한 연구개발 조직은 크게, 한국전자통신연구원(ETRI)를 위시한 정부출연 연구소와 『모바일 보안기술 연구회』와 같은 민간출연 연구소, 정보보안에 특화하는 주요 대학 연구소, 그리고 민간 기업체의 연구개발 부서/연구소의 세 그룹으로 나누어 볼 수 있다. 민간 기업체의 경우는, SKT와 KT 중심의 모바일 네트워크 사업자, LG-CNS 등 주요 SI 사업자와 안철수 연구소를 위시한 순수 민간 보안솔류션 개발자로 대별되어 질 수 있다. 각 연구개발 조직은 전체 정보보호 기술 중에서 관심과 특화하는 분야가 다르고 모바일 보안분야에 집중하는 정도도 다르기 때문에 여기서는 국내의 대표적인 모바일 보안기술 연구 조직인 한국전자통신연구원의 연구개발 활동을 중심으로 모바일 보안기술 연구개발에 대한 현황과 전망을 하기로 한다.

2009년초 WIPI 폐지가 스마트폰 시장의 활성화에 기여하였지만, 현재 WIPI 폐지에 따른 국내 스마트폰 보안 취약점 및 위협에 대한 보안 기술 개발의 준비가 미비한 상태이다. 스마트폰 보안 기술은 PC 환경과 다르게 백신, 방화벽 등과 같은 단품형 기술을 적용하기에는 한계가 있다. 또한, 다양한 OS별 스마트폰 출시와 개방 정도의 차이 등으로 인해 각 기기 특성에 맞는 보안 소프트웨어 적용이 요구된다.

특히, 국내의 경우에는 인터넷 보안 서비스 환경이 ActiveX를 통해 대부분 이뤄지고 있기 때문에 스마트폰을 이용한 안전한 결제 서비스에 어려움이 있으며 PC 환경과 다르게 보안 서비스도 제한적으로 지원할 수 밖에 없는 실정이다. 안전한 스마트폰 서비스 환경을 보장하고 향후 발생 가능한 보안 위협에 대해 선제적 방어 체계를 구축하기 위해서는 단말 내부 보안기술과 더불어 원격 보안 관리, 안전한

결제 서비스 지원 및 앱스토어를 통해 배포되는 모바일 애플리케이션 검증 등의 기술이 필요하고, 국내외적으로 기술 초기 단계에 있는 스마트폰 서비스 보안 인프라 기술 개발이 요구된다

(1) 스마트폰 단말 보안 기술

사용자의 부주의로 인한 시스템 (노트북, 휴대 단 말등) 분실 혹은 외부 제 3자에 의한 시스템 도난 등을 통해 단말 복제, 도청 및 악용, 단말의 프라이 버시 데이터 보호 위협, 악성 코드 삽입 등의 보안 위협은 여전히 해결되지 않은 숙제로 남아 있다. 일반적으로 소프트웨어는 하드웨어에 비해 쉽게 조작될 수 있기 때문에 물리적 보안성을 제공해주는 MTM (Mobile Trust Module)을 이용하여 외부 공격으로부터 데이터, 키, 인증서 등을 안전하게 보호하고, 스마트폰 단말 플랫폼의 무결성 검증을 통해 악성 코드 실행을 사전 에 탐지하여 차단함으로써 보다 향상된 보안 기능을 제공할 수 있다.

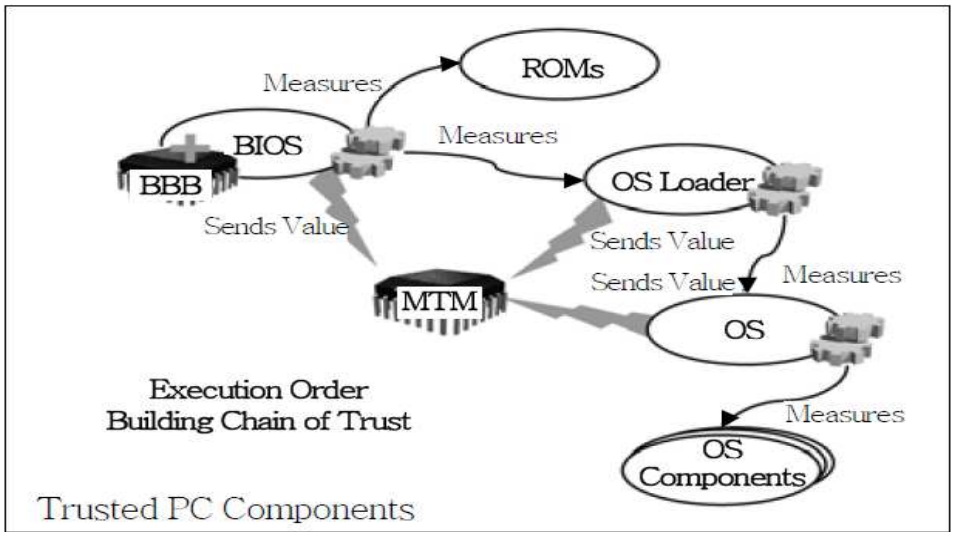
Root of trust 기능을 제공해주는 MTM 은 tamper-resistant 컴포넌트로써 데이터를 안전하게 저장하는 RTS(Root of Trust for Storage), 시스템 상태를 신뢰할 수 있는 방법으 로 증명하는 RTR(Root of Trust for Reporting) 역할을 담당하며, 시스템의 상태를 PCR(Platform Configuration Register)에 기록하는 RTM(Root of Trust for Measurement) 역할은 CRTM(Core RTM)이 담당한다. CRTM은 power-on 시에 가장 먼저 실행되고, 항상 신뢰할 수 있는 컴포넌트로 PC의 경우 BIOS에 포함될 수 있으며 임의로 수정할 수 없는 특징을 갖는다.

[그림 3-7]은 스마트폰 단말 플랫폼의 무결성 측정 과정을 보여준다. 단계별로 이루어지는 각 컴포넌트 별 무결성 측정 점은 chain of trust라고 보통 불리는데 일례로, CRTM이 BIOS의 무결성을 측정하고 결과 값을 검사하여 안전하다고 판단되면 MTM에 결과 값을 저장한 후 제어권을 BIOS에 넘긴다. 이후 BIOS는 동일한 방법으로 메모리, OS 등의 무결성을 측정하고 결과 값을 검사한 후 이상이 없을 경우

MTM에 결과 값을 저장한 후 제어권을 OS에 넘긴다.

이와 같은 무결성 검증 기능을 통해 OS 로드 후 MTM이 탑재된 스마트폰 상에서 악성 모바일 응용 프로그램을 실행하려 할 때, 별도의 IMVA(Integrity & Verification Agent)가 항상 동작하면서 RIM(Reference Integrity Metric) Certificate를 이용하여 해당 응용 프로그램의 무결성을 측정하고 검증하기 때문에 악성 코드 및 바이러스, 불법 프로그램들은 스 마트 폰상에서 실행될 수 없게 된다.

[그림 3-7] MTM Chain of Trust

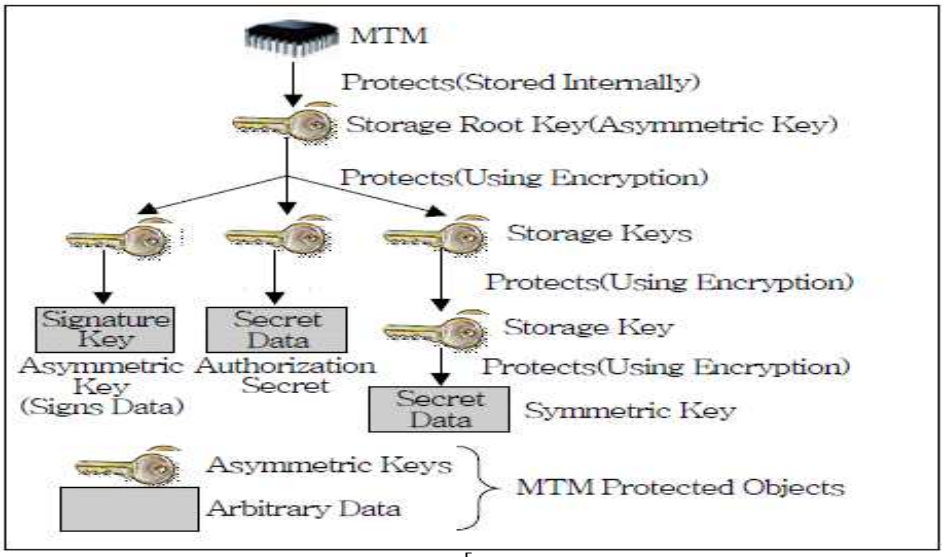


또한, MTM은 중요한 데이터 및 키를 외부로 절대 유출시키지 않으며, MTM 내에 데이터나 키를 저장할 수 있는 공간이 부족할 경우 SRK(Storage Root Key)를 이용하여 MTM 외부에 중요한 데이터나 키 값을 저장하는 protected storage 기능을 제공한다. [그림 3-8]을 보면 모든 key는 parent key로 암호화되어 계층적 구조 형태로 저장되며, 특정 key를 사용하기 위해서는 해당 key와 parent key가 MTM 내의 key slot으로 로딩된 후 해당키를 MTM 내에서 복호화 한다. 즉, SRK의 private 값은 MTM 외부로 절대 유출되지 않기 때문에 MTM 내에 안전하게 저장되어 있는 SRK를 통해 MTM 외부에 데이터나 키 값을

보다 안전하게 저장하여 사용할 수 있다.

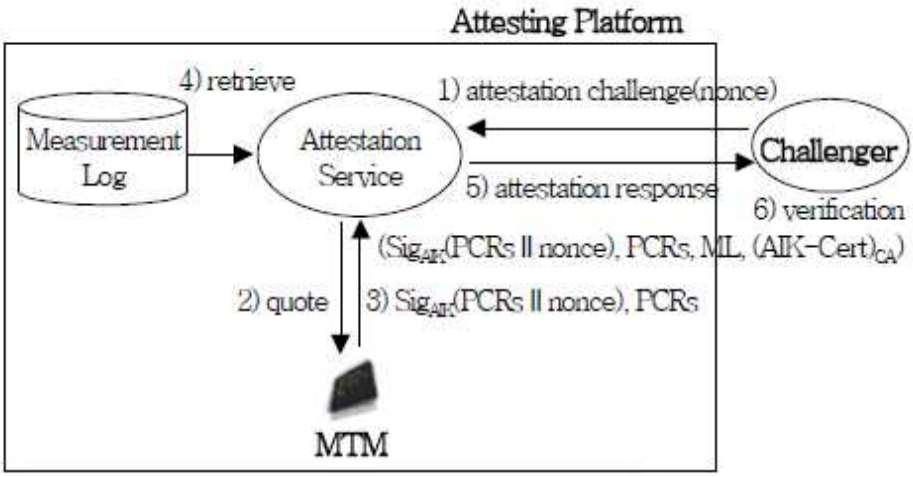
플랫폼이 신뢰할 수 있는 상태임을 다른 플랫폼에게 증명하기 위해 사용되는 remote attestation 과정은 [그림 3-9]와 같다. Challenger는 remote attestation 과정을 통해 신뢰할 수 있는 MTM이 스마트 폰 플랫폼에 장착되어 있으며, 현재 증명하고자 하는 스마트 폰 플랫폼의 상태가 안전한지를 Privacy-CA(Certification Authority)와 AIK(Attestation Identity Key) 및 AIK certificate를 이용하여 검증할 수 있다. 결론적으로, 앞서 기술한 MTM의 무결성 측정 및 검증 기능, protected storage를 통해 스마트폰 단말 보안 기능을 강화하고, remote attestation을 통해 MTM이 장착된 플랫폼들간의 플랫폼 보증을 통해 보다 안전하고 신뢰할 수 있는 무선 네트워크 환경을 구축할 수 있을 것이다.

[그림 3-8] MTM Protected Storage



[

[그림 3-9] MTM Remote Attestation

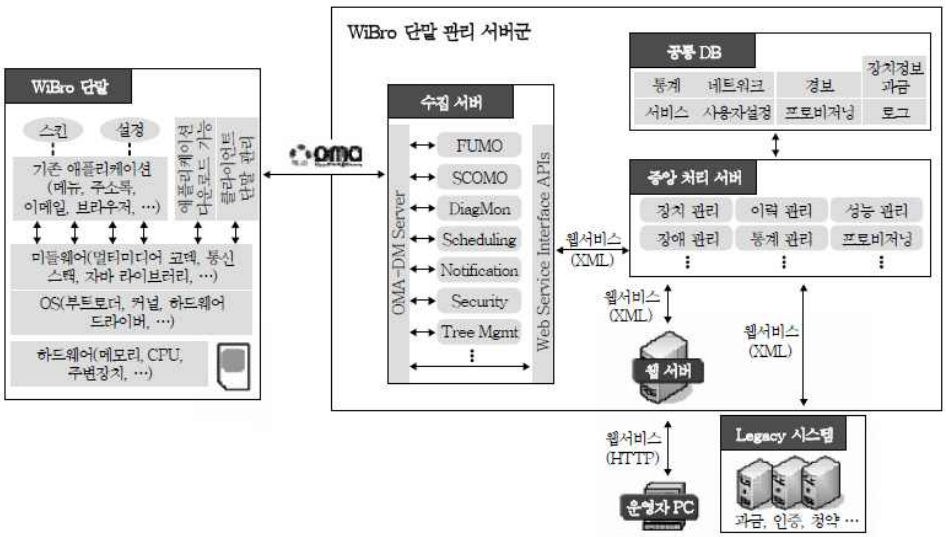


(2) 스마트폰 보안 관리 기술

원격 보안 관리 기술은 단말 관리 프로토콜을 사용하여 모바일 단말의 보안기능을 원격에서 제어하고 관리하는 기술이다. 이를 위해 모바일 서비스 표준화 단체인 OMA(Open Mobile Alliance) 에서 정의한 DM(Device Management) 프로토콜을 사용할 수 있다. DM 프로토콜은 두 통신 상대가 장치 관리 서비스를 제공하는 서버와 장치 관리 서비스를 받아 처리하는 클라이언트 관계를 갖는 프로토콜이다. 장치 관리 서버의 역할은 클라이언트에게 장치 관리 명령을 요청하고, 클라이언트는 주어진 명령을 수행한다. [그림 3-10]는 WiBro 단말 관리 시스템 구성도의 예를 보이고 있다. 현재 OMA DM은 단말 잠금과 데이터 삭제 기능을 정의하고 있다. 따라서, 이러한 기능을 스마트폰에 적용할 경우 보안 관리적 측면에서 장치 관리 서버는 스마트폰 보안 관리 서버의 역할을 담당하고, 클라이언트는 스마트폰에 설치하여 다양한 원격 보안 관리 서비스를 제공할 수있다. OMA DM 프로토콜은 HTTP, Wireless Session Protocol, OBEX 등의 전송 프로토콜과 바인딩 규격들이 마련되어 있으므로 산업계 인터넷 표준인 Web 환경, WAP

환경, 블루투스 환경에서 프로토콜 메시지 전송이 가능하다

[그림 3-10] WiBro 단말 원격관리 구조



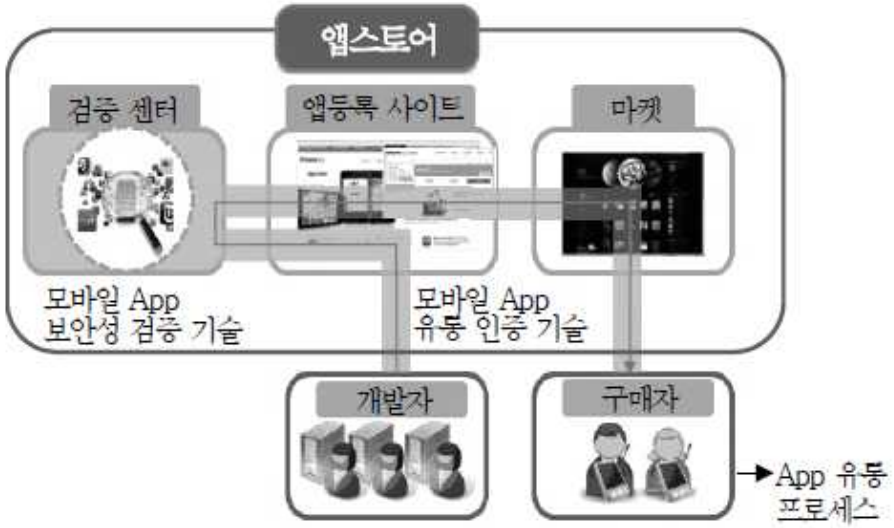
(3) 앱스토어 보안 기술

개방형 모바일 환경의 변화 및 개방형 플랫폼 도 입으로 스마트폰 기술 및 시장에 많은 변화가 이뤄 지고 있고, 방형 모바일 단말에 일부 악의적인 개 발자가 악성코드가 포함된 프로그램을 제작 및 유포해서 단말에 침해를 가하거나 개인정보를 습득할 수 있는 위협이 발생되고 있다. 현재 대부분의 앱스토 어에서는 등록된 애플리케이션의 심의 및 안전성 검증을 수동으로 진행하거나 보안을 위한 검증 절차가 이뤄지지 않고 있다. 이로 인해 앱스토어를 통해 다운로드받은 애플리케이션에 악성코드가 존재하는지 확인하는 데 한계가 있다. 실제 정보유출 공격을 수행하는 악성코드가 인터넷 뱅킹 관련 애플리케이션으로 은닉되어 앱스토어에 등록 및 배포된 사례가 발생되었다.

앱스토어에 애플리케이션을 등록하고 배포시, 애 플리케이션의 안전성을 확보하기 위해서는 모바일 애플리케이션의 유통 인증 기술과

앱스토어에 등록 된 애플리케이션에 대한 보안 검증 기술의 적용이 요구된다 ([그림 3-11] 참조).

[그림 3-11] 앱스토어 보안 기술



모바일 애플리케이션의 유통 인증 기술은 애플리 케이션이 앱스토어에 등록되어 구매자에게 전달되 기까지 유통자 증명을 제공하는 기술로써 이를 위해 코드 사이닝 (code signing) 기술을 적용하고 있다. 개발자는 개발한 모바일 애플리케이션의 신원증명 을 위해 인증서로 코드 사이닝하여 앱스토어에 등록 하고 앱스토어에서는 해당 애플리케이션에 대한 신 원증명을 확인하여 개발자 확인 절차를 수행한다.

일부 앱스토어에서는 공인인증서를 통한 코드 사이닝(Code Signing)을 적용하고 있지만 자가 서명 (self-signing) 이나 코드 사이닝을 적용하지 않는 앱스토어가 대부분이다. 따라서, 개발자 신원 증명 부재에 따른 악성코드 유포자의 확인이 불가능한 사례가 발생되고 있다. 개발자의 신원증명을 위해서는 공인인증서를 이용 한 애플리케이션 코드 사이닝 기법을 적용하여 개발자 신원 증명 절차가 요구된다. 모바일 애플리케이션 보안 검증 기술은 앱스토어에 등록된 애플리케

이션에 대해서 마켓 등록 전에 검증 센터에서 보안성 검사를 통해 애플리케이션의 안전성 여부를 확인하는 절차를 의미한다. 검증센터 에서는 애플리케이션에 대해서 역공학 (reverse engineering) 기법 및 가상 시험을 통해 보안성 검사를 진행하여 애플리케이션의 이상 유무를 확인하는 절차를 수행한다.

(4) 스마트폰 전자결제 기술

온라인 상에서 주로 사용되는 결제 수단은 신용 카드, 무통장 입금, 실시간 계좌이체, 휴대폰 결제 등이다. 이러한 결제 수단 중 무통장 입금이나 휴대폰 결제는 스마트 폰에서도 쉽게 적용될 수 있다. 그러나 스마트 폰에서 신용카드의 사용이나 실시간 계좌이체는 공인인증서 사용의 문제로 인하여 최근까지 본격적으로 활성화 되지 못했는데, 이는 전자금융 거래에서 30 만원 이상 거래금액일 때 공인인증서를 사용해야 하는 의무 규정이 준수되어야 했기 때문이다.

현재 국내 대부분의 웹 사이트에서는 공인인증서를 통한 전자서명을 지원하기 위해 쉽게 구현하여 사용할 수 있는 ActiveX 기술을 이용하여 전자서명을 제공하고 있다. 이 기능은 웹브라우저의 플러그인 형태로 동작하게 된다. 그러나 이러한 방식은 국내 전자거래 환경이 마이크로소프트의 기술에 종속되는 결과를 가져왔다는 논란을 야기하였다. 스마트폰이 확산됨에 따라 오픈웹 등에서는 전자결제를 위한 보안 기술로 기존의 공인인증서를 이용한 전자서명 기술뿐 만 아니라, SSL과 OTP를 이용하는 기술도 사용할 수 있도록 해 것을 요구한다.

이에 따라 방송통신위원회 등에서 전자금융 거래시 공인인증서 이외에도 '공인인증서와 동등한 수준의 안전성이 인정되는 보안방법을 도입할 수 있도 하였다. 이에 따르면, 30 만원 이상의 전자 거래에서는 공인인증서나 또는 공인인증서에 준하는 안전성을 평가 받은 기술이 사용될 수 있으며, 30 만원 미만의 소액 결제에 대해서는 공인인증서를 사용하지 않아도 된다. 이에 따라 스마트폰을 이용한 전자거

래시 기존 공인인증서뿐만 아니라 다양한 보안 기술이 전자결제시 활용될 것으로 보인다.

현재 국내에서는 하나은행이 최초로 아이폰에서 동작하는 스마트폰 뱅킹을 구현하였으며, 이에 대한 대응으로 타 은행들의 경우 은행권 공용 애플리케이션을 개발하고 있는 상황이다. 최근에는 은행권 공용 애플리케이션과는 별도로 각 은행별로 스마트폰 뱅킹 애플리케이션을 개발하고 있다. 이외에도 예스 24 등과 같은 인터넷 전자상거래 웹 사이트들의 경우 스마트폰에서 신용카드결제가 가능한 모바일 안심클릭 서비스를 제공하고 있다. 최근에는 NFC 를 탑재하는 스마트폰에 신용카드를 발급하여 비접촉식으로 대금을 지불할 수 있는 결제 기술도 개발중에 있다.

그러나 현재 개발되고 있는 스마트폰 전자결제 기술은 초기단계 상태로 스마트폰에서 사용자가 전 자결제 기능을 사용할 수 있도록 해주는 데 초점이 맞추어져 있다. 또한 전자결제 기술들이 상호 독립적으로 개발되고 있어 결제 기술은 사용자에게 일관 된 경험을 제공하지 못해 혼란과 불편을 가중시킬 수 있다. 따라서 향후 개발될 스마트폰 전자결제 기술은 사용자의 개인 행동 패턴에 기반하여 최적의 결제 수단을 자동으로 선택해주는 기능을 제공할 필요가 있으며, 전자결제 기술로 공인인증서뿐만 아니라 이 에 준하는 다양한 보안 기술을 통합적으로 제공하여 전자결제 애플리케이션의 특성에 맞는 보안 기술이 자동으로 제공될 수 있도록 해야 한다.

(5) 스마트 오피스 보안 기술

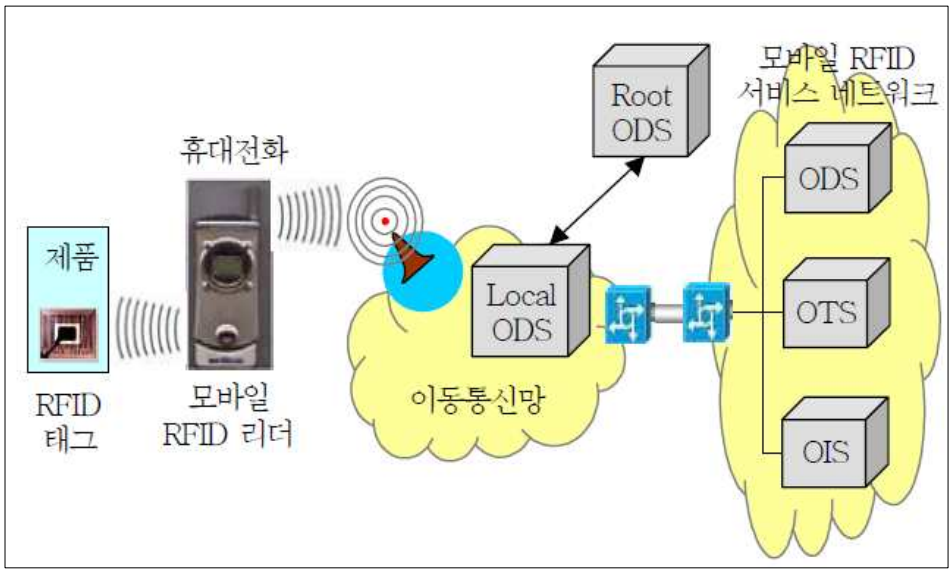
지금까지 스마트폰 보안 위협 요소와 모바일 악성코드 동향을 살펴보고 이들 위협에 대응하기 위한 단말 및 모바일 보안 인프라 기술들을 소개하였다. 스마트폰 확산에 따른 무선 인터넷, 앱스토어를 이용한 애플리케이션 활용 및 모바일 전자결제 서비 스 등 급격한 환경 변화에 맞춰 보안위협 및 장애요 인에 대응하기 위해서는 정부와 산학연간의 종합적 이고 체계적인 대응 방안이 요구된다. 안전한 스마

트폰 서비스 환경을 보장하고 향후 발생 가능한 보안 위협에 대해 선제적 방어 체계를 구축하기 위해서는 단말 내부 보안기술과 더불어 원격 보안 관리, 안전한 결제 서비스 지원 및 앱스토어 를 통해 배포되는 모바일 애플리케이션에 대한 검증 기술이 요구된다 국내외적으로 기술 기 단계에 있는 스마트폰 서비스 보안 인프라 기술은 스마트폰 서비스 산업 활성화를 도모할 수 있을 것으로 예상 된다.

(6) 모바일 RFID 보안 기술

모바일 RFID는 개인의 휴대전화에 RFID 리더 기능을 추가하여 RFID 서비스를 개인별로 특화시킬 수 있는 기술로서 모바일 RFID 서비스는 우리나라에서 이동통신 인프라를 바탕으로 휴대전화를 이용하여 사물과 사람 사이의 직접적 정보소통 관계를 제공하기 위하여 시작된 융합 서비스이다. [그림 3-12]은 모바일 RFID 시스템 개념도이다.

[그림 3-12] 모바일 RFID 시스템 구조도



[그림 3-12]의 모바일 RFID 서비스 네트워크에 존재하는 ODS 서버는 RFID 태그 식별자와 관련된 제품정보가 있는 OIS 서버의 위치를 알려주는 역할을 하며, OTS 서버는 개인 사용자에게 제품의 유통 정보 또는 OIS 서버의 이력을 제공하는 역할을 하며, OIS 서버는 RFID 태그 식별자와 관련된 제품의 주요 정보를 저장하고 관리하는 역할을 한다. 이러한 서버들과 휴대전화와의 통신은 이동통신망을 통해 수행된다. [그림 3-12]의 구성요소에 맞춰 모바일 RFID 서비스 제공을 설명하면 다음과 같다. 휴대전화를 소유한 개인 사용자가 휴대전화에 장착된 RFID 리더로 제품에 부착된 RFID 태그로부터 식별자를 읽는다. 휴대전화는 이동통신망을 통해 태그 식별자를 ODS 서버로 전달하여 태그 식별자와 관련된 제품정보를 가진 OIS 서버의 위치를 파악한다

2. 해외 주요 모바일 보안기술 연구개발

(1) 소프트웨어 방식의 한계

2009년 12월 아이폰용 스마트폰 뱅킹 서비스를 시작으로 다양한 금융서비스가 스마트폰을 통해 제공되면서 백신 소프트웨어, 키보드 보안 등 PC에 준하는 보안대책이 적용됐다. 하지만 스마트폰의 특성과 소프트웨어가 갖는 한계가 맞물려 예상치 못한 문제점들이 계속 발견되고 있다. 리버스 엔지니어링(Reverse Engineering)을 통해 탈옥이나 루팅된 폰의 금융서비스 이용 통제를 우회하거나 금융서비스 애플리케이션 위변조, 보안프로그램의 강제 종료 및 삭제 등이 이러한 예다. 리버스 엔지니어링을 방지하기 위해 소스^코드 암호화(일명 난독화) 프로그램을 사용하고, 애플리케이션 위변조 방지를 위해 배포 및 설치, 실행 전 인티그리티 체크(Integrity Check) 기능을 구현하며, 보안프로그램외 보호를 위해 워치독(Watch Dog) 기능을 구현할 수 있지만 스마트폰의 특성상 이러한 기능들을 완벽히 구현하는데 한계가 존재하는 것이다.

최근 인텔(Intel)이 맥아피(McAfee)를 인수해 시큐리티 프로세서 개

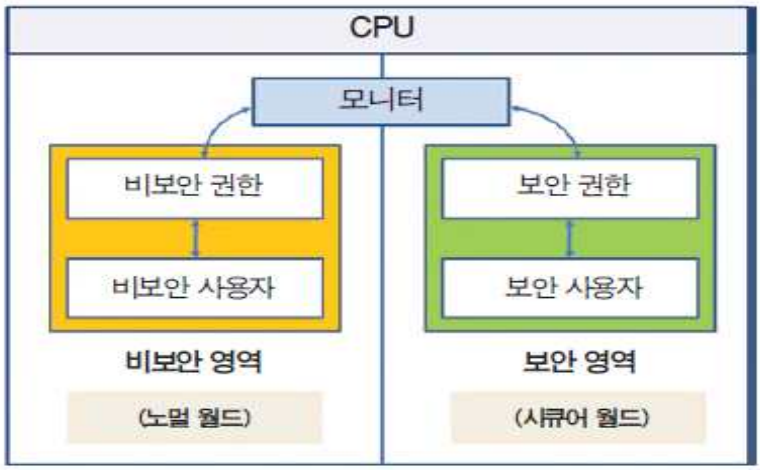
발을 추진하고 있으며, ARM(Advanced RISC Machine)사에서 제공하는 시큐리티 프레임워크인 트러스트 존(Trust Zone)을 이용해 보안솔루션을 개발하려는 움직임이 국내외에서 활발하게 이뤄지고 있다. 이는 소프트웨어 기반의 솔루션은 보안솔루션 자체가 해킹 공격을 받을 수 있고, 물리적 공격에 대응이 불가능하며, 리소스 한계에 따른 성능저하가 우려되므로, 소프트웨어의 일부 기능(또는 모듈) 또는 전부를 하드웨어 칩에 구현, 보안성과 성능을 높이기 위함이다.

하드웨어 칩에는 방화벽관과 파워센서, 온도센서 등의 안전장치가 마련돼 있으며, 파워센서는 연산과정 중에 소모되는 전류에 이상이 있을 경우에 이를 즉각 감지하며, 만약 데이터를 유출해 내기 위한 미세 전류가 흐르게 되면 파워센서가 이를 감지해 방화벽을 기동함으로써 이를 차단한다. 엑스레이로 데이터를 빼내려고 할 때는 엑스레이에서 발생되는 열을 온도센서가 탐지해낸다. 이렇게 하드웨어 칩은 데이터를 해킹할 수 없도록 물리적인 안정장치를 강화하고, 암호 가속기(Accelerator)를 내장해 RSA나 ECC 연산을 보다 빠르게 처리할 수 있다는 장점이 있다.

(2) 하드웨어 기반의 보안 솔류션

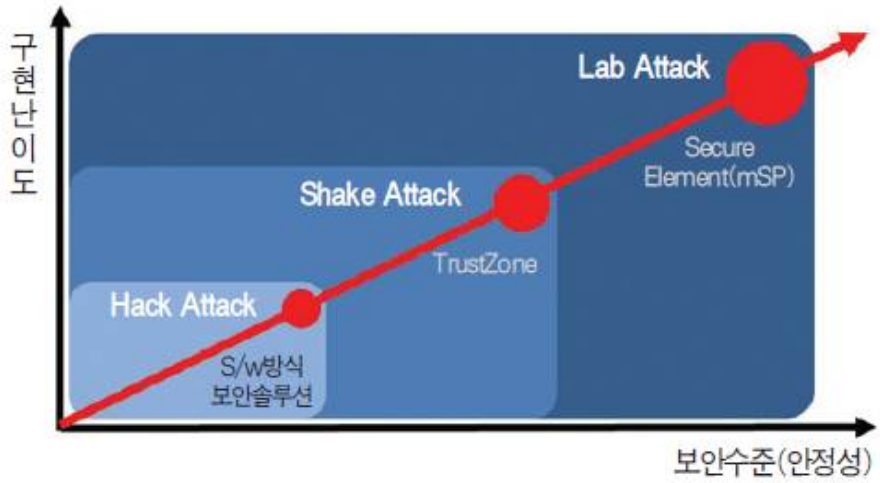
트러스트 존은 ARM사에 의해 개발된 기술로 코어텍스-A 계열의 CPU1에 적용돼 있다. 트러스트 존은 CPU를 노멀 월드(Normal World)와 시큐어 월드(Secure World) 2개의 독립된 영역으로 나누어 노멀 월드라 불리우는 비보안 영역(Nonsecure domain)에는 비보안 사용자(Nosecure User)가 비보안 권한(Nonsecure Privilege)을 사용하고, 시큐어 월드라 불리우는 보안 영역(Secure Domain)에는 보안 사용자(Secure User)가 보안 권한(Secure Privilege)를 사용하도록 설계돼 있다.

[그림3-13] Trust Zone Architecture



트러스존 기술을 이용해 솔루션을 개발하는 회사에는 G&D (Giesecke & Devirient), 트러스티드 로직(Trusted Logic) 등이 있으며, 대표적으로 보안 키패드(Secure Keyboard), 보안 스토리지(Secure SD Card)), 클라이언트 인증(Client Authentication) 등의 기능을 트러스트존 API를 이용해 사용할 수 있도록 구현돼 있다. 기존의 소프트웨어 방식 보안 솔루션이 멀웨어(Malware)나 바이러스, 그리고 소프트웨어 공격과 같은 핵 어택(Hack Attack)에 대한 방어를 수행한다면, 트러스트 존은 한 단계 높은 로우 버짓 하드웨어 어택(Low Budget Hardware Attack) 방식이나^JTAG(Joint Test Action Group)과 같은 물리적인 디바이스 액세스 공격 등 삭 어택(Shack Attack)에 대한 방어가 가능하다. 그러나 트러스트 존은 시간과 비용, 그리고 도구 사용에 제한이 없는 디스어셈블 디바이스나 엑스레이, 로직 프로브(Logic Probe)와 같은 랩 어택(Lab Attack)는 한계가 있다. 궁극적으로는 랩 어택까지 방어 가능한 시큐어 엘리먼트(Secure Element: 안전을 위해 별도로 설계된 하드웨어 칩을 의미, 모바일 시큐리티 프로세서 등이 이에 해당)가 가장 안전한 보안 솔루션 구현 방식이라 할 수 있다.

[그림3-14] 보안기능 구현난이도와 보안수준

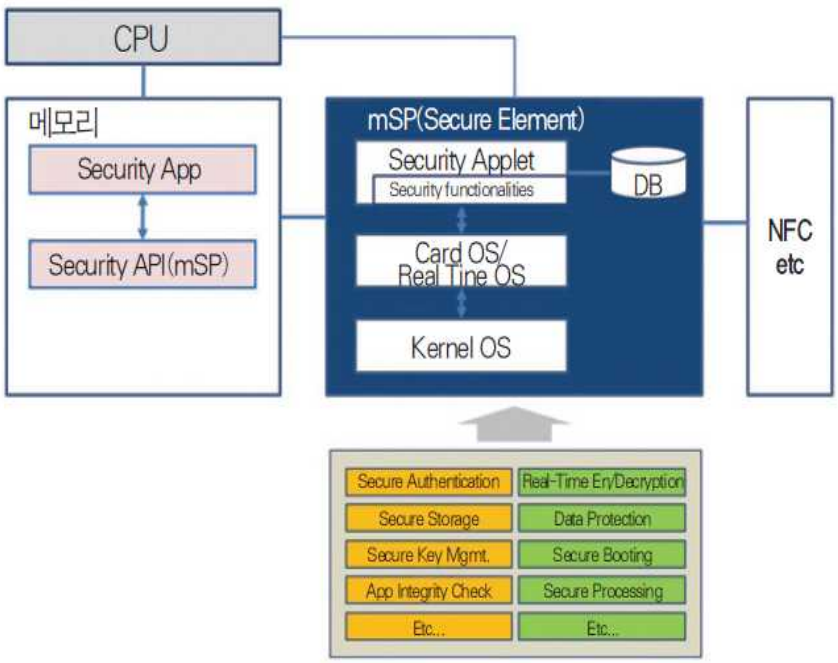


(3) 하드웨어 기반 보안 기술 전망

2010년 11월 프랑스 파리에서 열린 2010년 C&I (Cartes & Identification) 전시회에서 S사는 스마트 폰이나 태블릿 PC 등에 탑재할 목적으로 mSP(mobile Security Processor)를 개발중에 있다고 발표해 주목 받았다. mSP는 랩 어택에 대한 방어가 가능한 시큐어 엘리먼트로 복제가 거의 불가능한 스마트 카드 칩이라는 물리적인 보안체계 안에 정보보호 솔루션을 탑재해 2중 보안체계를 구현함으로써 모바일 환경에서 가장 안전한 보안체계를 구축할 수 있도록 한다. mSP는 직접 채널을 연결하고, 시큐리티 연산이 가능한 프로세서를 내장한 고성능/고속/대용량 보안 칩으로, 32 ~ 50 Mbps의 고속 데이터 전송속도 및 기가 바이트 이상의 대용량 저장공간, 멀티 쓰레딩 등을 지원하며, 소프트웨어 방식의 보안 솔루션으로는 한계가 있는 리버스 엔지니어링(Reverse Engineering) 및 애플리케이션 위변조, 보안프로그램의 강제 종료/삭제 등의 보안 위협을 완벽히 차단할 수 있다. mSP는 모바일 커머스 등 다양한 응용으로의 확장이 가능하도록 스마트 카드 OS를 탑재하고, 근접통신(NFC: Near Field Communication)와 연동이 되

는 구조를 기본으로 한다. 또 리얼타임 OS를 사용, 가볍고 슬림하며 파워풀한 보안 기능을 구현하도록 만들 수도 있다. 하드웨어와 융합된 보안 솔루션은 스마트 폰 출시 전에 먼저 탑재 돼야만 동작되는 강력한 보안기능(커널 레벨 및 관리자 권한으로 동작하는 기능 등)과 OS에 의존해 구현이 어려웠던 보안 기능을 보다 쉽게 구현할 수 있는 환경을 제공한다. 따라서 이들 시큐리티 프로세서가 본격적으로 출시될 1~ 2년 후에는 보다 안전하게 스마트폰과 모바일 오피스를 이용할 수 있을 것으로 기대된다.

[그림 3-15] mSP Architecture



제4장 모바일 보안 생태계와 상생 프레임워크 구축

제1절 모바일 생태계 개관

1. 정보통신 생태계의 변화

스마트폰 가입자 2천만 시대가 열렸다. 5천만 인구의 40%가 스마트폰을 쓰고 있다. 특히 경제활동인구 2천500만명의 80%가 스마트폰을 활용하면서 '스마트 라이프 혁명'을 이끌고 있다. 방송통신위원회는 지난 28일(2011년 10월 28일) 오후 우리나라 스마트폰 가입자가 2천만을 돌파한 것으로 추정한다고 30일 발표했다. 지난 27일 스마트폰 가입자 수가 1천998만명으로 집계돼 28일 오후 2천만을 넘어선 것이 확실해 보인다. 스마트폰 가입자는 지난 2009년 11월 아이폰 도입 시 47만명에서 올해 3월 1천만명을 넘어섰다. 아이폰 도입시기부터 약 2년이 걸렸다. 방송통신위 이상학 통신정책기획과장은 "이제 국민 10명중 4명이 스마트폰을 이용하며 경제활동인구 2천500만명의 대부분이 스마트폰을 이용하는 셈이 된 것"이라며 "우리가 스마트폰 도입은 미국과 유럽에 비해 늦었지만 가장 빠르게 가입율이 늘어나는 국가"라고 설명했다.

스마트폰 확산은 우리의 일상생활을 변화시키고 있다. 사람들은 스마트폰으로 정보를 얻고, 이메일을 주고받으며 업무를 한다. 소셜네트워크 서비스로 사회적 관계를 형성하고, 각종 애플리케이션으로 여가 활동에 활용한다. '스마트 라이프 혁명'의 바람을 맞고 있다. 지금까지 휴대폰은 음성통화 수단이었지만, 스마트폰은 편리한 생활을 동

반자이자 하나의 '종합 문화서비스 플랫폼'으로 자리잡고 있는 것. 김영세 이노디자인 대표는 최근 아이뉴스24가 주최한 디지털커뮤니케이션컨퍼런스에서 "스마트폰은 또다른 나이자, 세상을 보는 창"이라며 커뮤니케이션의 핵심 수단이라고 의미를 부여했다.

스마트폰과 태블릿PC 등 '스마트 기기'들은 일상 뿐만 아니라 정보통신기술(ICT) 산업의 지형도 바꾸고 있다. 통신서비스의 중심이 음성에서 데이터로 급격히 넘어갈 뿐만 아니라 스마트폰 확산은 기존 서비스 중심의 ICT 시장이 플랫폼과 단말기 중심으로 변화 확대하는 경향을 보이고 있다. 스마트폰이 기업의 생산·영업 활동에도 크게 기여하고 있다. 포스코(제조공정, 안전관리)나 도시철도공사(현장시설물 관리, 고장신고·접수가)가 스마트폰을 산업 현장에 도입했고, 현대조선소도 축구장 800개 크기의 조선소 현장을 4세대 LTE 기반의 스마트워크 시스템으로 바꾸고 있다. ICT 업계는 이같은 변화의 물결이 90년대 후반의 유선인터넷 확산으로 인한 벤처 붐과 유사한 형태의 새로운 벤처 붐 을 촉발할 것으로 기대하고 있다. 클라우드컴퓨팅과 사물통신(M2M) 확산으로 ICT 시장의 새로운 사업기회도 늘어날 것으로 예상하고 있다. 업계 관계자는 "소셜네트워크서비스(SNS), 위치기반서비스(LBS), 근거리통신(NFC) 등의 새로운 서비스가 금융, 유통, 전자상거래 등 다양한 분야에서 혁명적 변화를 이끌고 시장을 활성화할 것"이라고 기대했다.

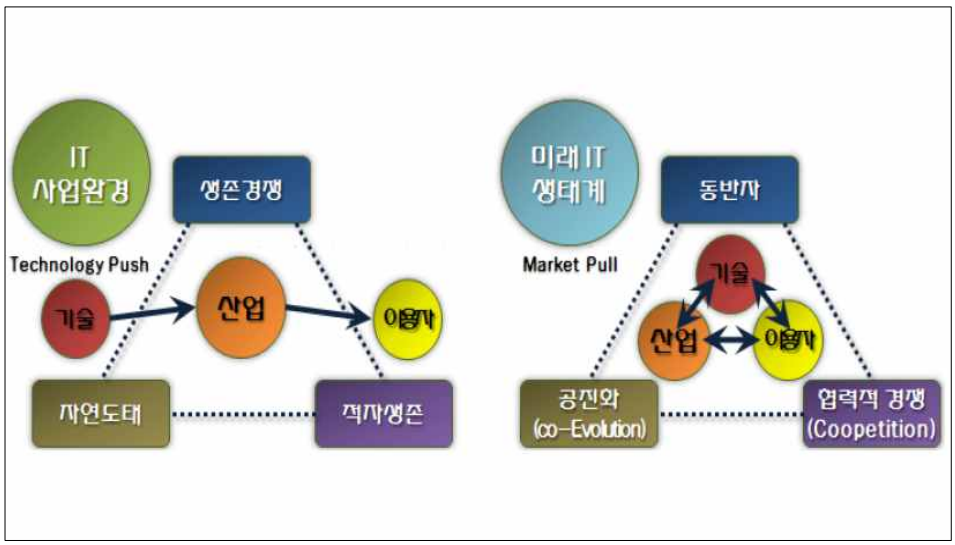
특정 산업의 가치창출 구조를 규명하려는 이론적 논의는 지속적으로 발전되어왔다. 1985년 마이클 포터의 가치사슬(value chain) 이론으로부터 시작하여 보다 복잡하게 분화되고 빠르게 전개되는 환경을 분석하는 도구로서 가치 네트워크(value network), 비즈니스 생태계(business ecosystem) 이론 등이 전개되어 왔다. 이러한 가운데, 초기의 마이클 포터 이론을 기반으로 한 가치사슬 모형이 다양하게 분화되면서 산업의 가치 창출 구조를 설명하는 데 유용하게 사용되었다. 그러나 제품 가치(product value)보다는 네트워크 가치(network value)로, 협력적 경쟁(coopetition) 및 공진화(co-evolution)의 중요성이 커지는 환경에서는 생태계 개념이 보다 유용하다는 분석이 제기되고 있

다. 특히 Fransman(2010)에 의해 제기된 ELM(ecosystem layer model)은 생태계의 공생적 관계를 설명하는 모델로 많이 도입되고 있다.

여기서 생태계는 이론적으로 공동의 운명 하에서 하나 이상의 자원을 공유하고 공진화(co-evolve)하는 기업체 및 개인의 집단(Moore, 1996), 어떤 환경 내에서 상호 작용하는 다수의 유기체들의 집합(Fransman, 2007), 지역적 한계가 없고 경쟁과 협력 메커니즘을 동시에 가지면서 상호 운명을 공유하도록 자생적으로 연결된 커뮤니티(Peltoniemi, 2004)를 의미한다. 즉, 생태계는 가치사슬상 다른 단계에 속하는 기업들이 상호보완적인 공생(symbiotic) 관계를 통해 효율적 생산과 혁신이라는 공동의 목표를 달성하는 분산형 생산 및 혁신 시스템(complementary innovation, distributed creativity)을 의미하는 것이다.

이러한 생태계의 개념은 네트워크·웹(network·web) 형태의 관계를 강조하고 정적 선형의 관점이 아닌 종합적인 동태적 시각(holistic dynamic view)을 제공한다 ([그림 4-1]). 이 이론은 제품에 내재된 가치만이 중요한 것이 아니라, 전체 네트워크상의 가치도 중요함을 주장하며, 환경적 변수를 포괄하고, 진화의 개념을 내포하고 있다.

[그림4-1] 전통적/경쟁적 IT 생태계 대 공생적/공진화적 IT 생태계



이 그림은 전통적인 경제•경영 이론상에서의 기업경쟁과 가치창출 흐름이 생태계 관점에서 공진화, 협력적 경쟁, 동반자 등의 개념으로 변화하고 있으며, 기술, 산업, 이용자가 일방적인 흐름이 아닌 서로에게 긴밀한 영향을 주고 받고있음을 나타내고 있다.

2. 모바일 생태계의 탄생

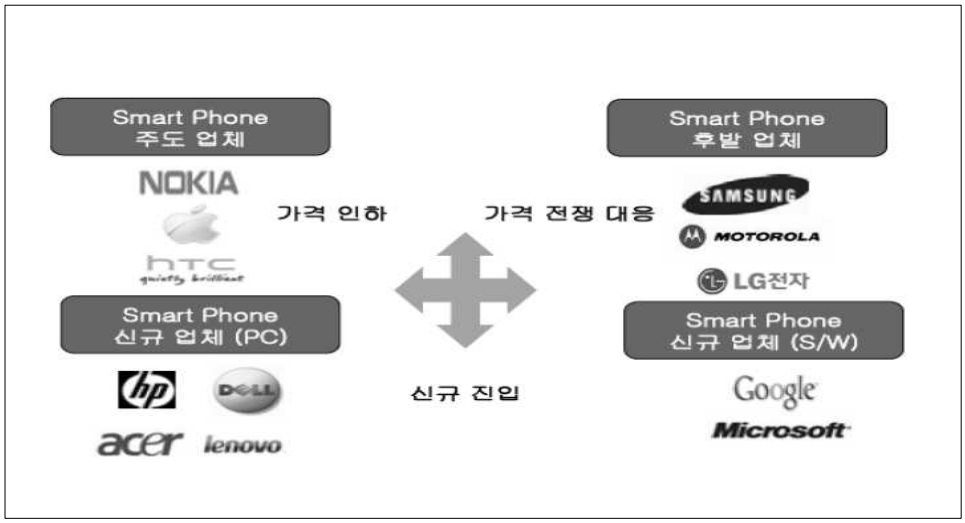
최근 방송통신시장의 산업구조가 가치사슬과 같은 산업구조에서 생태계로 진화하고 있는 것으로 분석된다. 이러한 분석은 스마트폰의 도입 및 성장과 더불어 주파수와 네트워크를 독점적으로 이용하며 가치를 창출하던 이동통신사업의 가치창출 구조가 변화하고 있다는 사실에 근거한다. 즉, 기존의 분석도구인 가치사슬상의 다른 단계에 속하는 다양한 기업들이 상호 보완적인 공생(symbiotic) 관계를 통해 효율적인 생산과 혁신을 추구하며, 공동의 목표를 달성하는 분산형 생산 및 혁신이 나타나고 있으므로 가치사슬보다는 생태계로 파악하는 것이 적절하다는 것이다.

이동통신 분야가 모바일 생태계(Mobile Ecosystem)의 형태로 진화하고 있다는 대표적인 사례로는 애플(Apple)과 구글(Google)이 창출한 가치창출의 구조가 거론되고 있다. 이들 기업들은 독점적인 주파수와 네트워크를 기반으로 이동전화를 제공하던 이동통신사업자와 단말업체의 영향력을 크게 약화시키며, 새로운 형태의 비즈니스 모델을 구축하였다. 애플, 구글 등이 주도하는 혁신에 따라 이동통신은 전통적인 통신사업에서 비통신을 포괄하는 모바일 생태계로 발전하고 있다.

이러한 모바일 생태계의 형성과정에서는 스마트폰 등 스마트 디바이스의 확산과 독자적인 OS(Operating System) 또는 플랫폼의 확보가 중요한 동인으로 작용하고 있다. 이에 따라 주요 기업들은 OS(Operating System)를 중심으로 독자적인 생태계를 창출하기 위해 노력하는 동시에 다양한 스마트 디바이스의 개발을 모색하고 있다. 현재까지 애플이 iOS를 기반으로 아이폰, 아이패드를 출시하며 이동통신시장을 선도하는 가운데, 독자적 OS를 보유하지 못한 사업자들은

개방형인 구글의 안드로이드(Google) 기반 스마트폰 OS에 참여하고 있다. 국내의 경우, 삼성전자가 구글의 OS을 기반으로 하는 안드로이드폰 생산에 주력하면서도 독자 플랫폼(Bada)의 개발을 통한 다변화를 시도하고 있다. 아래의 [그림 4-2]는 디바이스를 중심으로 한 스마트폰 시장경쟁 양상을 경쟁전략을 중심으로 도식화하여 제시하고 있다.

[그림 4-2] 스마트폰 시장경쟁 양상

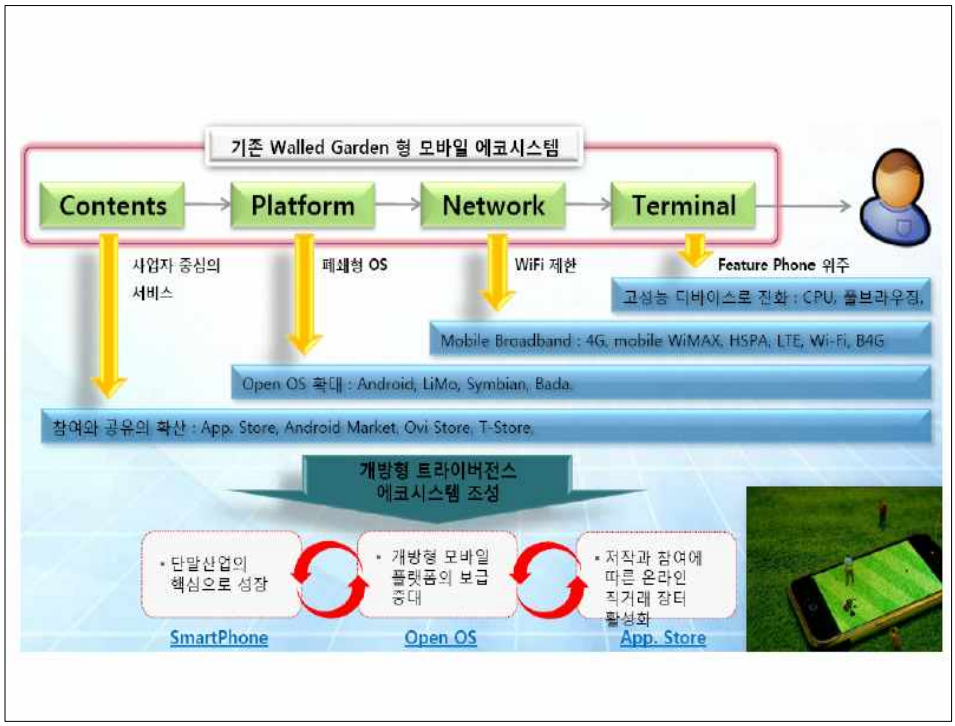


모바일 생태계의 형성과정에서 가장 주목할 변화는 폐쇄형 및 수직형 가치사슬에서 개방형 모바일 생태계로 변화하고 있다는 점이다. 새로운 모바일 생태계에서는 스마트폰을 비롯한 단말산업, 독자적 OS를 기반으로 하는 플랫폼, 온라인 직거래 장터인 앱스토어 활성화가 매우 중요한 경쟁요인으로 나타나고 있다. 아래의 [그림 4-3]은 개방형으로 진화하는 모바일 생태계의 변화를 나타내고 있다.

이와같이 모바일 시장에서 생태계(mobile ecosystem)는 모바일 서비스의 가치창출에 기여하는 핵심 요소들 간의 관계를 설명하기 위한 도구적 개념으로 생태계는 과거에 하나의 지배적 사업자(dominant player)에 의해 주도되는 수직적 공급체제에서 분업화된 생산자들의

직렬 구조를 설명하기 위해 사용되었던 가치사슬(value chain)이란 개념으로부터 발전하였다.

[그림 4-3] 모바일 IT 생태계의 변화



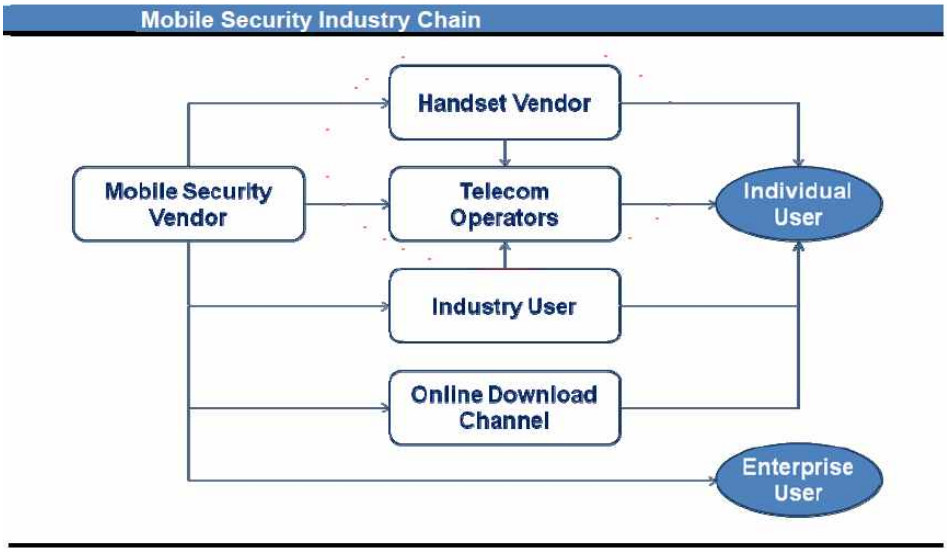
구체적인 예로 애플은 혁신적인 UI(User Interface)를 기반으로 한 단말의 경쟁력, 음원 등과 같은 다양한 콘텐츠 사업자들과의 협력에 기초한 플랫폼 중심의 콘텐츠 거래환경 조성을 통해 글로벌 모바일 인터넷 생태계를 주도하고 있다. 그리고 구글은 OS 개방, 이통사에 대한 콘텐츠 수익분배 등의 개방성을 기치로 단말제조사, 이통사와의 협력을 통해 안드로이드 플랫폼을 확산시키고 있다. 결과적으로 애플, 구글과 같은 혁신 기업을 중심으로 개방형 모바일 생태계의 형성이 이루어진 이후 이동통신의 가치창출 구조는 개방형 모바일 생태계의 선순환 구조를 달성하는 방향으로 더욱 강화되는 추세이다.

제2절 모바일 보안산업 가치사슬 및 생태계 분석

1. 모바일 보안 산업의 가치사슬 분석

최근 각종 새로운 모바일 보안문제가 대두되자 더 많은 수의 모바일 보안제품 제조사들이 관련제품을 잇따라 선보이며 시장에 참여하고 있어 해당 분야의 산업 가치사슬이 단계적으로 형성되고 있다.

[그림 4-4] 모바일 보안산업 가치사슬



Source: Frost & Sullivan

[그림 4-4]에서 보는 바와 같이 모바일 보안 산업 가치사슬에는 대부분의 모바일 통신사업 참여자들이 연계되어 있으며, 현재는 보안제품 제조사와 WAP 및 모바일 보안제품 제공을 위해 WAP 및 인터넷을 통해 확장중인 채널들간의 공조 양상이 크게 나타나고 있다. 모바일 보안제품 제조사들은 통신사 및 휴대전화 제조업체들을 포함한 산

업사슬 내 참여자들과의 관계를 토대로 협력에 나서고 있으며, 이동통신사업자들이 그 중심에 있다. 상이한 양상을 보이는 다양한 협력 모델을 아래 간략히 소개한다:

■ 모바일 보안업체 –> 온라인 다운로드 채널 –> 개별 사용자:

현재 사용자들이 유료 및 무료 모바일 보안제품을 확보하는 주요 채널은 인터넷, WAP, BBS, 앱스토어 등을 통한 온라인 다운로드다. 이 가운데 다운로드 수를 기준으로 보면 인터넷과 WAP가 가장 보편적으로 이용되고 있으며, 앱스토어의 경우 모바일 보안제품 영역에 있어 아직 탐색 단계에 있는 관계로 홍보에 대한 투자가 비교적 적은 편이다. 다만 해당 분야 앱스토어 개발이 진행될수록 홍보도 그만큼 강화될 것으로 기대된다. 보안업체들은 온라인 다운로드 외에도 대형 모바일 매장을 통한 소프트웨어 패키지의 형태로도 자사제품을 판매하고 있으나 이러한 형태는 아직까지 명백한 효과를 거두지는 못하고 있다.

■ 모바일 보안업체 –> 이동통신사 –> 개별 사용자:

보안업체와 이동통신사가 상호 광범위하고 긴밀한 협력관계를 유지하는 방식이다. 우선 모바일 보안업체가 이동통신사에서 취급하는 단말기에 보안용 소프트웨어를 사전 설치하는 경우가 있다. 스마트폰의 수가 늘어날수록 통신사가 자체 개발해 탑재하는 보안 자원은 물론 사전 설치를 위한 모바일 보안제품을 주문하는 경우도 증가할 것으로 보인다. 둘째로는 보안업체가 이동통신사측에 모바일 보안기능을 제공하는 형태를 들 수 있으며, 셋째로는 보안업체가 이동통신사의 네트워크 레이어 보안에 협력하는 형태를 들 수 있다. 이 경우에는 보안업체가 이동통신사 애플리케이션 스토어의 안전성 확보를 위해 각기 다른 개발자들이 업로드하는 소프트웨어를 검사하는 방식의 모델을 취한다.

■ 모바일 보안업체 –> 모바일 단말기 제조사 (–> 이동통신사) –> 개인 사용자:

보안업체가 단말기 출고시점부터 모바일 단말기 제조사에 보안용 소프트웨어를 제공하는 모델이다. 노키아의 심비안, 구글의 안드로이드 등과 같이 주요 스마트폰 제조사들은 고유 OS 플랫폼을 보유하고 있고 OS 개방화 추세에 맞추어 전세계적으로 다양한 형태의 앱이 써드-파티 개발자들에 의해 개발될 것으로 예상되나, 이윤을 목적으로 한 모바일 바이러스 및 악성 소프트웨어 개발자들의 유입을 완벽히 차단할 수는 없기에 잠재적 위험요인이 존재한다. 따라서 스마트폰 제조가 급증하는 만큼 단말기 제조사가 사전 설치할 수 있는 보안 SW 수요도 늘어날 것으로 전망할 수 있다. 이러한 모델은 이미 적용되고 있어 주요 모바일 보안업체와 대형 단말기 제조사가 고객 보안성 향상을 목표로 협력중인 사례가 존재한다. 통신사가 보안 SW를 사전 설치한 맞춤형 단말기를 확보할 수 있게 된다면 통신사의 입장도 유리해질 수 있으며, 다른 한편으로는 보안업체와 단말기 제조사, 통신사 모두가 처음부터 내장형 보안 SW 개발에 공조하는 형태로도 발전할 수 있다.

■ **보안업체 -> B2B 사용자 (-> 이동통신사) -> 개인 사용자:**

모바일 앱은 금융, 웹사이트, 써드-파티 결제 플랫폼 및 각종 모바일 기반 결제 등 다양한 영역에 걸쳐 개발되므로 보안업체가 시중 은행과 협력하거나 PayPal과 같은 써드-파티 결제 플랫폼과의 공조체제를 통해 고객 계좌의 비밀번호 보안을 강구하는 방안도 가능하다. 또는 하드웨어 플랫폼에 안정된 보안제품을 제공할 수 있는 네트워크 장비 제조사가 통신사업자에 그러한 솔루션을 공급하는 방식도 가능하다.

■ **보안업체 -> 기업 사용자:**

모바일 보안업체들은 아직 기업 사용자들과의 완전한 협력단계까지 영역을 확장시키지 못했으며, 주된 이유는 업무용 스마트폰의 낮은 보급률로 인해 대다수의 기업이 임직원들의 휴대전화를 통한 기밀정보 유출의 잠재적 위험을 크게 인식하지 못하고 있기 때문이다. 따라서 기업용 모바일 보안제품에 대한 수요 발굴에는 좀더 시간이 걸

릴 것으로 예상되지만, 스마트폰 자체의 확산과 업무용 기능의 증가에 따라 기업용 모바일 보안제품 시장이 대폭 확대될 것으로 예상되므로 모바일 제조사들은 기업용 수요를 면밀히 지켜볼 필요가 있다.

2. 모바일 보안에 대한 통신사업자의 수요 분석

2009년 이후 통신사업자들의 부가가치 서비스(VAS)는 줄곧 원활한 성장세를 보이고 있어 전반적인 수익성 증대에 핵심 역할을 수행하고 있다. 차이나 모바일의 경우 2010년 1분기 VAS 사용자수가 5억 1천만 명으로 전년 대비 9.7% 증가했고 SMS 사용량도 전년 동기대비 2.3%의 상승률을 기록했으며, SMS를 제외한 다른 서비스의 이용도 계속해서 늘어나고 있다. 통신사들은 스마트폰과 3G 통신망이 보편화됨에 따라 결제, 위치정보, 앱스토어, IM, 원거리 모니터링 등 각양각색의 모바일 앱을 다량 출시하며 전략적으로 사업을 추진하고 있다. 그와 동시에 앱 기반 비즈니스 플랫폼의 보안 강화 부문에도 점차 관심도를 높여가고 있다.

아래에서는 모바일 결제 분야를 지목해 통신사업자들의 보안 수요를 파악해보고자 한다. 현 시점에서 모바일 결제에는 크게 두 가지 방식이 존재한다:

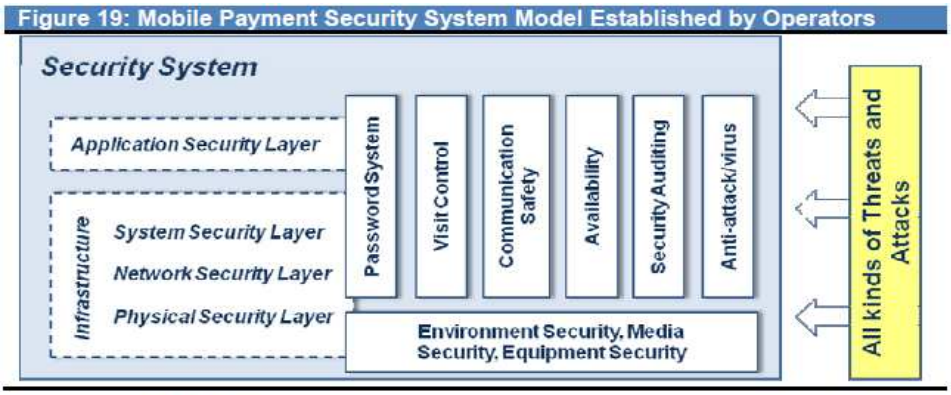
1. 추가 하드웨어 보완: RFSIM과 같은 유관 하드웨어를 모바일 기기에 내장시킴으로써 SIM 카드에 RFID 기능을 추가해 하나의 SIM 카드로 다양한 유형의 결제가 가능하도록 하거나, NFC 모듈을 탑재함으로써 모바일 결제를 구현하는 방식이다. 상기 방식들은 모바일 결제에 있어 커다란 위험요인을 내재하고 있는데, 바로 사용자의 계정정보와 모바일 정보가 서로 동기화되어 존재한다는 점이다. 즉 모바일 휴대기기를 분실할 경우 개인정보를 어떻게 보호할 것인지가 커다란 향후 과제다.

2. 인터넷 기반 결제: WAP 네트워크, SMS 인증, 또는 써드-파티 결제 플랫폼을 사용해 무선 결제를 구현하는 방식이다. 일례로 PayPal

의 경우 오랜 시간 검증된 결제 시스템을 갖춘 써드-파티 결제 플랫폼을 운영해오고 있으며, 결제 기능을 갖춘 모바일 클라이언트를 휴대전화 사용자들에게 제공하고 있다. 온라인 결제 솔루션과 RFSIM/NFC의 뚜렷한 차이는 바로 추가 하드웨어의 존재 유무다. 통신사업자들은 3G 통신망을 적극적으로 홍보하며 모바일 결제 부문에도 상당한 관심을 기울이고 있으나, 아직까지 보안 문제를 완전히 해결하지 못한 상태다. 인증용 SMS 역시 손쉽게 해킹이 가능하며, 바이러스의 공격에도 여전히 취약하다. 따라서 모바일 결제의 보호에는 보안용 SW 제품의 추가 적용이 반드시 고려되어야 한다. 이에 따라 통신사업들은 [그림 4-5]에 드러나있듯 이전보다 공격적으로 모바일 결제용 보안 시스템 모델을 구축하고 있다.

모바일 결제용 보안 시스템은 인프라 계층과 애플리케이션 보안계층의 두 층위로 나뉜다. 인프라 계층의 보안은 곧 물리적 보안계층과 네트워크 보안계층 및 시스템 보안계층의 확보만을 의미하며, 이를 바탕으로 반드시 애플리케이션 보안 계층이 구축되어야 한다. 애플리케이션 보안계층은 암호 시스템 관리, 방문기록 관리, 송수신 보안, 가용성, 보안 감사 및 각종 위협과 공격에 대비한 백신 등 다방면에 걸쳐 이루어진다.

[그림 4-5] 네트워크 사업자의 모바일 결제용 보안 시스템



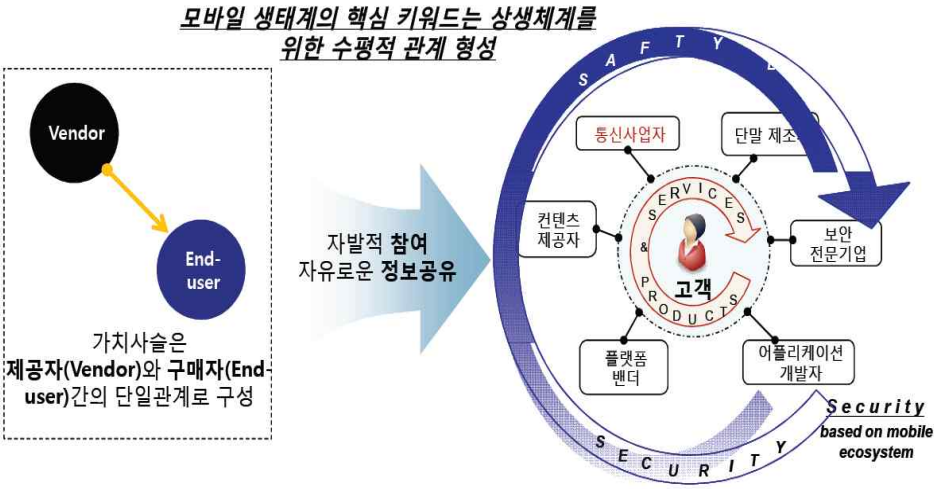
Source: Frost & Sullivan

제3절 국내 모바일 보안 산업 육성을 위한 정책적 고려사항

1. 모바일 보안 시장과 상생 프레임워크

모바일 생태계의 주요 구성요소는 콘텐츠(Contents), 플랫폼(Platform), 네트워크(Network), 단말기(Terminal)로 구성되며, 모바일 생태계는 전통적인 수직적 생태계에서 확장형, 융합형 생태계로, 개방형 글로벌 생태계인 스마트 생태계로 진화하고 있다. 이에따라 콘텐츠, 플랫폼, 네트워크, 단말기 부문 사이의 수평적 협력 및 경쟁을 통한 생태계의 혁신이 발생하고 있다.

[그림 4-6] 모바일 보안 생태계 상생 프레임워크



모바일 보안 생태계에 있어서 핵심개념은“플랫폼”이다. 플랫폼은 ICT 시장에서 다양한 의미로 사용되고 있는데, 최근 휴대폰 시장

에서 스마트폰의 등장과 함께 플랫폼의 경쟁 양상은 하드웨어에서 소프트웨어 중심으로 전환되고 있다. 디바이스가 지능화되고 컨버전스로 인해 복잡해 지면서 PC 수준의 관리기능이 요구되고 있다. 상황에 따른 신속한 정보처리 기능, 융•복합화에 따른 시스템 안정성 확보, 사용자 인터페이스 개선 등을 위해 PC가 아닌 다른 디바이스에서도 PC에서와 같은 플랫폼이 필요하다. 앞으로는 휴대폰, PDA, 태블릿 PC 등 휴대용 기기의 소프트웨어 플랫폼을 모바일 소프트웨어 플랫폼 또는 줄여서 모바일 플랫폼이라고 부르도록 한다.

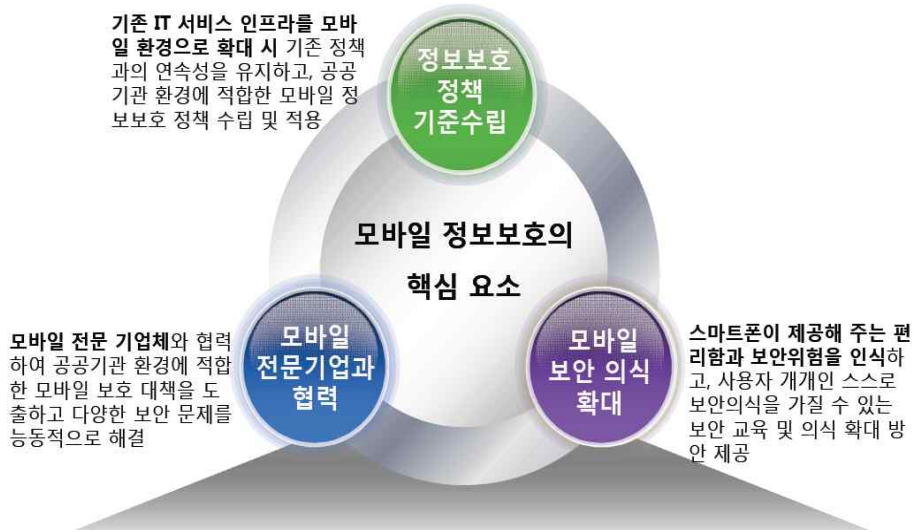
모바일 소프트웨어 플랫폼은 기존의 모바일 소프트웨어 개발업체의 수익 구조를 변화시킬뿐만 아니라, 향후 무선 인터넷 서비스 및 모바일 기기에서의 애플리케이션과 콘텐트에 대한 의존도를 높임으로써 이동통신사업 전반의 가치시스템의 구심점으로 작용하여 모바일 생태계(ecosystem)의 핵심 역할을 수행할 것으로 기대된다.

우리나라 모바일보안 산업의 가장 큰 약점은 그 가치사슬에 참여하는 산업계의 상호협력 또는 자생적 생태계가 안정화되지 않았다는 것이다. 모바일 보안대책이 문제발생시마다 즉흥적 대책이 아닌 구조적이고 조직적인 해결체계를 가지기 위해서는 국가적인 차원에서 모바일 보안 생태계 구축이 시급하고 스마트폰 보급 확산단계인 지금이 모바일 보안 생태계 형성과 대책 수립의 적기라고 생각되며 특히, 우리나리 모바일 보안전반을 고려한 모바일 전자정부 도입은 모바일 생태계 발전에 큰 역할을 제공하는 선순환 구조의 시발점이 될 것이다. 즉 모바일 정보보호의 핵심 요소 확립으로 모바일 서비스 사용환경을 위한 정보보호 기반을 강화할 수 있다는 것이다. 이를 위해 지금까지의 기존연구는 주로 모바일보안에 관련된 개별적인 참여자의 개별적인 대책과 해결책을 제시하는데 머무르고 있는 한계를 가지고 있다.

모바일 보안 생태계 구축을 위해서는 어느 한 영역·분야에서의 보안 대책 수립만으로 진정한 의미의 모바일 보안 생태계 구축이 어렵다. 본 연구에서는 제시하는 상생 프레임워크는 다음의 [그림 4-7]에서 보여지고 있다. 이의 구현을 위해서는 모바일 보안과 관련된 모든 영역·분야에서 상생적/상호

보완적인 모바일보안 산업생태계 구축을 지원할 수 있는 정부차원에서의 대책이 필요하다.

[그림 4-7] 건강한 모바일 정보보호 생태계 구축



2. 건강한 모바일 보안 생태계 구축을 위한 정책적 고려사항

그러면 우리나라가 21세기 지구촌의 새로운 키워드인 디지털 융합과 유비쿼터스 사회에 있어서 핵심인 모바일 소프트웨어 플랫폼과 모바일 보안산업의 경쟁력을 확보하기 위해 국가적으로 어떤 전략을 택해야 하는가? 본 보서고의 앞 절에서 본 것처럼 소프트웨어 플랫폼 기반의 다면 플랫폼 시장은 관련된 산업 네트워크들이 서로 밀접하게 상호 작용하면서 하나의 생태계를 형성하여 진화해 간다. 이렇게 어떤 플랫폼을 중심으로 관련 산업 네트워크가 밀접하게 상호작용하며 움직이는 산업 생태계가 국가적 차원의 경쟁력을 가지기 위해서는 무엇보다도 정부차원에서 지향해야 할 바른 방향의 지표들을 설정하는 것이 중요하다. 이러한 정책지향 목표에는 여러 가지가 있을 수 있으나 여기서는 S. Greenstein가 제시한 네 가지 지표를 중심으로 소개하고자 한다(Greenstein (2010)). S. Greenstein이 제시한 네 개의 지표는

경제적 실험(Economic Experiments), 경쟁적인 표준들(Standards Competition), 창의적 기업가 정신(Inventive Entrepreneurship), 그리고 일방적 협상의 부재 (Absence of One-sided Bargaining)이다.

첫째, 경제적 실험이 풍부해야 한다. 경제적 실험이 풍부하면 그 산업생태계는 건강하다는 신호이고 부족하면 문제가 있다는 신호이다. 여기서 경제적 실험이란 한 기업이 잘 알려지지 않는 경제적 요인의 불확실성에 대하여 학습하거나 해결할 수 있도록 만들어진 시장지향적 행동(Market-oriented Action)이다. 예를 들어 지난 10년간은 차세대 인터넷 기술로서 Web 2.0 기술의 등장이 있었고 이 신기술에 대한 경제적 실험이 왕성하게 진행되어 왔다(미국의 경우). 우리는 이 신기술에 대한 경제적 실험을 성공적으로 이끌어 가고 있는 사례들 - Google, Facebook, Salesforce.com-이 있는 반면, 이렇게 성공한 사례보다 훨씬 많은 수의 실패한 사례들이 있다는 것을 알고 있으며, 이 신기술에 대한 경제적 실험은 계속 진행중이다.

물론 개별 기업이나 투자자에게는 개개의 실험결과가 중요하다. 그러나 사회전체적으로 보았을 때 더 중요한 것은 개개의 실험 결과가 아니라 이러한 경제적 실험으로부터 얻어지는 학습의 효과이다. 이러한 학습 효과는 암묵적 지식(Tacit Knowledge)으로 축적되어 산업생태계의 또 다른 중요한 무형적 기반인 사회적 자본을 형성하게 되는 것이다. 이러한 학습은 결코 실험실이나 통제된 환경에서는 제대로 배울 수없기 때문이다. 따라서 우리나라의 경우 대기업 위주의 IT 정책을 고수한다면 좋은 결과를 기대하기는 어려울 것이다. 대기업 집단의 소유주 기업가들이 경영권을 세습하는 환경에서는 이러한 경제적 실험과 그 효과를 사회적으로 기대하는 것은 어렵기 때문이다.

둘째, 왕성한 표준 경쟁이 있어야 한다. 앞에서 본 것처럼 플랫폼 기반의 산업, 특히 다면 플랫폼 기반의 산업은 연관된 산업 네트워크들로 구성된 산업 생태계를 이루기 때문에 혁신적인 산업 생태계에서는 종종 동종 플랫폼간의 격렬한 경쟁이 벌어지곤 한다. 이러한 플랫폼간 경쟁의 한 양상이 바로 표준 경쟁이다. 본 고의 중심 주제인 스마트폰이 바로 이 현상을 잘 보여주고 있다. 앞에서 본 것처럼 현재

스마트폰의 플랫폼 시장은 수 많은 플랫폼들간의 경쟁으로 채워져 있고, 이들 간의 경쟁은 표준 선점 경쟁으로 진행되어 갈 것이다. 이 경우 표준은 한 국가의 공식적 표준이나 ISO 등 국제표준과 같은 공식적 표준이라기 보다는 사설적 표준(Proprietary Standards) 또는 산업적 표준(Industry Standards)과 같은 사실적 표준(De Facto Standards)을 지칭한다. 스마트폰뿐만 아니라 현재 인터넷은 과거에도 그랬던 것처럼 수많은 표준들의 경연장이다. 특히 무선이동 통신망과 디지털 미디어 기술 분야에서 수많은 표준안들이 제안되고 있으며 이들의 경쟁 상태와 양상은 치열하고 다양하게 전개되고 있다.

물론 모든 표준이 항상 이렇게 경쟁 상태에 있어야 한다는 것은 아니다. IP, TCP, Ethernet, HTTP 등 인터넷 표준들은 일단 공식적 표준으로 이미 그 위치가 확고히 정립된 표준들이며 이들에 대한 개정 혹은 새로운 대체 표준은 이들이 처음 등장했을 때 대른 대안들과 치열하게 경쟁하여 현재와 같은 위치를 차지했던 바와 같이 그 과정을 밟아야 할 것이다. 경쟁없이 정립된 표준은 후에 표출될 많은 잠재적 문제점들을 내포하고 있는 경우가 많다. 대표적인 예가 PC와 웹브라우저 시장을 독점하고 있는 마이크로소프트사가 단독적으로 설정한, 인터넷에서 다운로드되어 브라우저내에서 실행되는 Active X를 들 수 있다. Acive X는 현재 특히 그 보안상의 취약점 때문에 많은 문제점을 일으키고 있지만 마이크로소프트사의 독점적 시장 지배력 때문에 많은 고객들이 피해를 입고 있다고 보여진다.

세 번째 지표는 창의적 기업가 정신이다. 창의적이고 진취적 기업가는 새로운 경제적 기회를 추구하는 조직을 이끌어 모험적이고 도전해 볼 만한 사업에 몰입한다. 이러한 기업은 수익을 올리는 것을 목적으로, 보다 넓은 (잠재적인) 고객층에게 더 낳은 새로운 제품 또는 서비스를 제공하는 데에서 누구도 해보지 못한 대담한 시도를 하는 적극적 참여자이다. 이러한 진취적 창의적 기업가에는 작은 규모의 벤처 기업은 말할 것도 없고 대기업에서도 시도할 수 있다. 이와 같이 창의적이고 진취적인 기업은 왕왕 기존의 대기업에 의해 흡수되기도 하고, 때로는 공개 과정을 거쳐서(IPO) 그들 자신만의 중견기업, 대

기업으로 성장하기도 한다.

창의적 기업가 정신을 북돋우는데는 세 가지 요인이 있는데, 낮은 개발 비용(Low Development Cost), 신속한 상업화 과정(Fast Speed to Commercialization), 그리고 생태계에 의해 결정되는 수익성 권리 전용의 용이성(Strong Appropriability Conditions as Defined by the Ecosystem)이다. 개발 비용은 보통 첫 번째 주요 자금조달이 이루어진 시점 또는 설립자가 주제품 개발 책임자를 임명한 시점에서부터 그 첫 주제품을 출시할 때까지 소요되는 총경비를 의미하고, 상업화 속도는 소요된 시간으로 측정한다. 수익성 권리 전용의 용이성이란 창의적 기업가가 비밀 유지, 특허, 저작권, 시장 선점자적 장점(First-mover Advantage) 또는 이와 같은 것들의 조합을 통해서 제3자의 모방을 방지하여, 그 자신의 새로운 혁신제품 또는 서비스, 또는 자신만의 유일한 자산에 대해 독점권을 유지할 수 있는 용이성을 지칭한다.

넷째, 마지막 지표는 일방적 협상의 부재이다. 기업과 기업가들의 일상은 수많은 크고 작은 협상의 연속이다. 대부분의 경우 이 협상은 동등한 지위(Peer-to-Peer)에서 진행된다. 그러나 어떤 협상은 협상의 균형추가 넘어져 일방적 협상(One-sided Bargaining)이 된다. 이러한 일방적 협상의 극단적인 형태는 한 쪽('갑')에서는 어떤 것을 요구하고 상대방 쪽('을')은 '갑'의 요구 조건을 거절하거나, 아니면 높은 댓가를 치르고 그 조건을 수용하든가 해야 한다. 이 극단적인 상황의 가장 단순한 발현은 시장에서 우위를 가진 쪽('갑')이 다른 당사자('을')에게 어떠한 다른 선택의 여지도 남겨주지 않으면서, "받아들이든지 아니면 말든지(Take-it-or-leave-it)" 오퍼를 선언할 때 발생한다.

왜 일방적 협상이 혁신적 환경을 위해서 나쁜 신호인가? 일방적 협상은 한 가지 큰 문제점을 보여주는데, 그것은 협상의 우위에 있는 쪽('갑')이 그들의 협상에서의 우위를 이용하여, 심지어 협상의 조건이 협상의 열위에 있는 쪽('을')의 부담과 희생을 수반하더라도 협상의 우위쪽에 유리하도록 정당화시키는 길을 제공하기 때문이다.

특히 일방적 협상이 협상 열위 쪽(을)에 치명적 손실을 끼치면서 우위에 있는 쪽의 어떤 방어적 목적으로 사용되기 시작하면, 그것은 경제생태계 전체의 혁신에 치명적 손상이 될 수 있다. 그것은 경제적 실험 행위(Economic Experiments)를 제한하고, 공평한 표준 경쟁으로부터 발생하는 사회적 혜택(Benefits from Standards Competition)을 원천적으로 발생 불가능하게 할 수 있다.

제5장 결 론

현재의 모바일 ICT 시장은 폐쇄적, 수직적 생태계에서 개방적, 수평적 생태계로 진화하고 있으며, 시장의 글로벌화가 진전되어 전통적인 네트워크 사업자 외에 콘텐츠, 단말기 부문에서 특히 해외 사업자의 시장 영향력이 증대되고 있다. 글로벌 모바일 ICT 사업자들은 플랫폼 경쟁에서 유리한 위치를 선점하기 위해 콘텐츠, 애플리케이션, 단말기 및 서비스 부문에서 치열하게 경쟁하고 있으며, 이는 특허 확보를 위한 M&A나 수직결합을 통한 기술의 내재화 등으로 다양하게 나타나고 있다.

모바일 ICT 생태계 변화에 따른 국내 기업의 전략적 포지셔닝(strategic positioning)의 목표는 경쟁 우위에 있는 부문의 역량 강화를 바탕으로 플랫폼 경쟁에 참여하여 실현 가능한 영역에서 플랫폼 지위를 획득하는 데 있다. 이는 우리나라 모바일 ICT가 네트워크 인프라는 세계 최고 수준이며, 단말기 제조업 부문에서 세계적인 경쟁력을 갖추고 있는 등 주로 하드웨어 부문에서 강점을 보이고 있으며, 스마트 생태계에서 핵심적인 부분이라 할 수 있는 콘텐츠 및 소프트웨어 부문에서는 세계 수준과 비교해 매우 취약한 경쟁력을 갖춘 것으로 파악된다.

생태계 관점에서 우리나라 모바일 보안산업을 발전시키기 위해서는 1) 수평적 생태계 조성, 2) 경쟁우위 산업 부문에 대한 경쟁력 유지, 3) 취약 부문의 성장 및 발전을 통한 생태계 균형 발전이라는 세 가지 차원에서 점검할 필요가 있다.

생태계의 수평화는 혁신을 위한 환경 조성에 가장 근본적인 요소로, 이를 위해서는 지배적 대형 사업자와 소형 협력사 간의 고질적인 불공정 거래의 관행을 개선시키는 것이 가장 중요하고 시급한 사안이다.

소프트웨어 부문에서의 경쟁력 강화를 통한 모바일 보안산업 생태계 균형 발전은 향후 ICT 시장에서 소프트웨어 부문의 중요성과 성장 가능성으로 미루어 보아 장기적 관점에서 반드시 중점적으로 간주해야 할 요소이다. 다만, 현재 우리나라의 소프트웨어 부문에서의 기술 경쟁력 및 시장 규모가 글로벌 시장에서의 선진국에 비해 뒤처지고 있는 현실을 고려하여 제도적 지원이 뒷받침될 필요가 있다. 규모가 작은 소프트웨어 기업들의 비즈니스를 활성화시키기 위해 M&A에 따른 청산소득금액에 대한 세율을 인하하거나, 초기단계에서의 기업 투자를 촉진하기 위해 엔젤 투자에 대한 세제 지원책을 마련하는 일, 그리고 인터넷 벤처 기업의 인력난 해소를 위해 병역특례 요건을 완화하는 등의 제도적 지원을 하는 것은 소프트웨어 관련 기업 육성에 긍정적으로 기여할 수도 있다.

참 고 문 헌

국내문헌

강동호 외 (2010), “스마트폰 보안 위협 및 대응 기술”전자통신동향분석 제25권 제3호.

공영일 (2010), “스마트폰의 함의와 시사점”, 정보통신정책, 제22권 4호 통권 480호.

김동기 (2010), “모바일서비스 미래 전략”, 《정보통신정책연구원 정책포럼 발표 자료》 2010. 10. 21.

나성현 외 (2010), 『국내 무선인터넷 생태계 선순환 구조 구축 방안 수립』, 한국인터넷진흥원 위탁연구보고서 2010년 12월 31일

모바일보안기술연구회 (2011), 『모바일 보안기술 수요와 전망』 《모바일 보안기술연구회 세미나 자료집》 2011년 9월 28일.

방송통신위원회 (2010a), “무선인터넷 활성화 종합계획”.

방송통신 위원회 (2010b), “Smart Korea 강국 도약을 위한 스마트 시큐리티 종합계획”.

유효선 (2011), "모바일 오피스 구현, 보안대책 마련이 최우선,” 《Network Times》 2011년 3월.

정동길 (2011), "한국의 휴대용 단말기 플랫폼 전략," 정보과학회지 제28권 제11호.

주재욱(2011), "ICT 생태계의 현황과 발전 전망"《정보통신정책연구원(KISDI) Premium Report》.

한국정보보호학회 (2011), 『모바일 보안 컨퍼런스 2011』 《한국정보보호학회 컨퍼런스 자료집 2011년 7월 6일》.

한국인터넷진흥원 (2011), 『2011 국가정보보호백서』 한국인터넷진흥원.

외국문헌

Chaouchi, Hakima and Maryline Laurent-Maknavicius, 『Wireless and Mobile Network Security: Security Basics, Security in On-the-shelf and Emerging Technologies』, Wiley, 2009.

Dujarric, Robert and Andrei Hagiu, "Capitalizing on innovation: The Case of Japan," Harvard Business School Working Paper 09-114, HBS, 2009.

Evans, David, Andrei Hagiu and Richard Schmalensee, Invisible Engines: How Software Platforms Drive Innovation and Transform Industries, Cambridge, MA: MIT Presss, 2006.

Frost and Sullivan, 『China Mobile Security Market Research Report』 Frost and Sullivan, 2010.

Greenstein, Shane, "Glimmers and Signs of Innovative Health in the

Commercial Internet," Journal on Telecommunicatiions and High Technology Law, Volume 8, Issue 1, 2010.

Hudson, Sally J. , "Mobile Security Market, Consumer and Corporate Concerns"International Data Corporation(IDC), 2011.

Weiser, Mark, "The computer for the 21st century," Scientific American, 265:94-04, September 1991.

Weiser, Mark & J.S. Brown, "Designing Calm Technology", PowerGrid Journal, volume 1.01, July 1996.

저 자 소 개

정 동 길

- 서울대 경제학과 졸업
- KAIST 산업공학과 석사
- 텍사스텍대 경영학과 박사
- 현 명지대학교 경영정보학과 교수

장 정 우

- 명지대 경영정보학과 졸업
- 현 한국IBM 연구원

오 민 진

- 중앙대 경영학과 졸업
- 중앙대 경영학과 석사

조 아 라

- 명지대 경영정보학과 졸업

방송통신정책연구 11-진흥-라-08

모바일 보안시장 생태계 조성을 위한 환경구축 연구

(A Study on Mobile Security Ecosystems)

2011년 12월 일 인쇄
2011년 12월 일 발행

발행인 방송통신위원회 위원장
발행처 방송통신위원회
서울특별시 종로구 세종로 20
TEL: 02-750-1114
E-mail: webmaster@kcc.go.kr
Homepage: www.kcc.go.kr
인 쇄 태광문화사